SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

1

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: AFIT/CI/NR 88-16	2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle): FEDERAL TELECOMMUNICATIONS SYSTEM 2000. A MILITARY PERSPECTIVE	5. TYPE OF REPORT & PERIOD COVERED: MS THESIS
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s): FRED W. HILLS	8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS: AFIT STUDENT AT: UNIVERSITY OF COLORADO	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS	12. REPORT DATE: 1988
	13. NUMBER OF PAGES: 163
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office): AFIT/NR, Wright-Patterson AFB OH 45433-6583	15. SECURITY CLASS. (of this report): UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

DISTRIBUTED UNLIMITED: APPROVED FOR PUBLIC RELEASE

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

SAME AS REPORT

18. SUPPLEMENTARY NOTES

Approved for Public Release: IAW AFR 190-1
LYNN E. WOLAVER 12 July 88
Dean for Research and Professional Development
Air Force Institute of Technology
Wright-Patterson AFB OH 45433-6583

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

ATTACHED

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

The Federal Telecommunications System 2000, a Military Perspective

The General Services Administration (GSA) is currently working on replacing the Federal Telecommunications System (FTS), a 25 year old network made of mostly AT&T leased analog switches and lines. Since the 1982 divestiture of the Bell System, the government has lost special tariff rates as well as ATT's technical expertise, making the FTS an expensive and burdensome operation. With technological advances such a digitization and integration of services, increased user requirements of value added services and a highly competitive marketplace, a replacement is needed to ensure continued government telecommunications operation up through the year 2000.

GSA, having analyzed these factors within the framework of fiscal realities, proposes the FTS2000 as the answer to the federal government's telecommunications problems. This system will offer voice, data and video services across a transparent, nationwide network. The winning bidder will assume all technical and operational responsibility for the network, providing the government with these state-of-the-art services according to each agencies needs.

What advantages does the FTS2000 have for the military that could offset all or part of the expense of building separate, dedicated networks? What policy decisions must be taken, no matter what system the military opts for, in the interest of national defense? How can the government ensure connectivity and interoperability of its agencies in an era of changing technological innovations? This thesis addresses these matters and proposes alternatives and policy that the military should consider with the advent of the FTS2000.

Fred W. Hills, Captain, USAF
Master of Science in Telecommunications
University of Colorado, Boulder, CO
1987
173 pages

THE FEDERAL TELECOMMUNICATIONS SYSTEM 2000

A MILITARY PERSPECTIVE

by

FRED WILLARD HILLS

B.S., Baylor University, 1979

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Master of Science

Program in Telecommunications

1987

This thesis for the Master of Science degree by

Fred Willard Hills

has been approved for the

Program in Telecommunications

by

Harvey Gates

Dale Hatfield

Russ Shain

Date December 1, 1987

Hills, Fred Hills (M.S., Telecommunications)

The Federal Telecommunications System 2000, a Military Perspective

Thesis directed by Professor Harvey Gates

The General Services Administration (GSA) is currently working on replacing the Federal Telecommunications System (FTS), a 25 year old network made of mostly AT&T leased analog switches and lines. Since the 1982 divestiture of the Bell System, the government has lost special tariff rates as well as ATT's technical expertise, making the FTS an expensive and burdensome operation. With technological advances such a digitization and integration of services, increased user requirements of value added services and a highly competitive marketplace, a replacement is needed to ensure continued government telecommunications operation up through the year 2000.

GSA, having analyzed these factors within the framework of fiscal realities, proposes the FTS2000 as the answer to the federal government's telecommunications problems. This system will offer voice, data and video services across a transparent, nationwide network. These services will be provided by contractor supplied facilities, eliminating major capital investments and risks of technological obsolescence to the government. The government will depend on industry's technical expertise and direction to provide state-of-the-art system to meet its needs. Finally, pricing of services will be based on usage,

giving every agency the opportunity to use all services for and reasonable price.

Even though most agencies endorse this plan, the military has backed out of the program and is presently pursuing a similar strategy to buy separate data and voice networks at greater cost. What advantages does the FTS2000 have that could offset all or part of this expense? What policy decisions must be taken, no matter what system the military opts for, in the interest of national defense? How can the government ensure connectivity and interoperability of its agencies in an era of changing technological innovations? This thesis addresses these matters and proposes alternatives and policy that the military should consider with the advent of the FTS2000.

To Barb and Sara

CONTENTS

TABLE

Table

FIGURES

Figure

ABSTAINER

This research represents the views of the author and does not necessarily reflect the official opinion of the U. S. Air Force, Department of Defense or other government agencies.

CHAPTER I

INTRODUCTION

The federal government's telecommunications needs are enormous as they are diverse. The General Services Administration (GSA) is tasked with the responsibility of ensuring these needs are met in the most efficient and economical way possible.

Since 1963, GSA has managed the Federal Telecommunications System (FTS) to provide government agencies nationwide with a reliable voice and slow speed data backbone. The FTS is made of dedicated analog switches and transmission lines, linking major cities across the US, including Alaska and Hawaii, Puerto Rico and the Virgin Islands. This system is managed by the government, with AT&T and other providers supplying leased facilities and technical staff. This arrangement was extremely effective in the stable telecommunications environment of the 1960's and 70's. However, technology, user's needs, and the marketplace have changed radically since then. Furthermore, current fiscal realities have made GSA reevaluate its role as the federal government's telecommuncitions provider.

Major technological changes are sweeping the telecommunications environment. The once separate and rival worlds of computers and telecommunications have now become one thanks to technology. This has given rise to the shift from analog to digital transmission as the preferred means of information transfer, be it voice or data. Furthermore, the advent of digital technizes and the resulting integration of user services has revolutionized the use of transmission media and switching techniques. These changes are summarized in Integrated Services Digital Networks (ISDN), an international standardization effort, which has the industry racing toward integration at an ever increasing pace.

The federal government's telecommunications needs have also expanded. In the 1960's and 70's, most agencies used voice traffic with limited need for slow speed data to carry out their day-to-day operations. But, in the mid to late 1970's, automation of services became an integral part of the government's transmission needs. The FTS, which was never intended to handle this type of traffic, is ineffective to carry these new loads. Therefore, federal agencies must seek alternate modes of transmission. The resulting diversity of systems within the federal government has led to inefficiencies and lack of interoperability, costly problems in an era of fiscal restraint.

Additionally, the telecommunications marketplace has become extremely decentralized and competitive. Between the loss of the FTS special tariff, TELPAK, and divestiture of the Bell Company in 1982, the federal government lost its cost and one-

stop service advantages. Numerous benefits did arise in the marketplace, however. As result of deregulation and expanding technologies, the market is wide open with vendors offering a diversity of services, both data and voice, and at competitive prices. The key is to figure out what services are needed and at what cost, difficult questions for the government who is now suffering from a shortage in technical expertise to make these decisions.

Recognizing these factors, GSA redefined the government's role in managing telecommunications resources. First, they realized the need to get a grasp on federal government's use of telecommunications to ensure interoperability and efficiency at an economical cost. The marketplace was now rich in services and through competition, GSA could get them at the right price. Additionally, recognizing their limited technical expertise in a dynamic field, GSA would need to transfer the operational and maintenance functions to the contractor. The government would now purchase services, letting the provider take care of capital investments such as facilities, hardware, software etc. This would leave GSA with the job they are best at, contract management. Finally, the contract would stipulate a steady migration to Integrated Services Digital Network (ISDN) standards, ensuring the government has the latest that technology has to offer, when it is offered.

The resulting architecture is the FTS toward the year 2000, or FTS2000. It will replace the FTS by the year 1990 and be the prime supplier of telecommunications services for the federal

government up to and beyond the year 2000. It is the largest undertaking of its type in the world. With a ten year life span and an estimated cost ranging from $4 to 25 billion, GSA would establish a nationwide network, revolutionizing telecommunications services within the federal government. The services offered include common user/dedicated voice, data and video, both in analog and digital formats. Also included in the contract are packet switching, electronic mail and eventual switched digital/integrated services. There will be no up-front capital investment by the government. The system provides the government with services and lets the contractor worry about the technical details. These services will be priced on usage, with each agency guaranteeing minimum usage levels.

With the advent of FTS2000, the US will have a major telecommunications resource at it disposal for conducting government business. Most federal agencies, including the Office of the Secretary of Defense and the Defense Communications Agency (DCA) have accepted this approach as a viable solution to their intergovernmental needs. The Department of Defense (DoD) as a whole has not. The Army, Navy and Air Force have all stated reasons for not wanting to be part of the project, yet have not turned it down completely as a future alternative. However, the military is now bidding for separate data and voice networks, using the same criterias as used with the FTS2000 selection, but at two to three time the cost of DoD's participation in the FTS2000 project. Additionally, by the military, a major telecommunications user, dropping out of the FTS2000 project,

certain economies of scale are lost, driving up the project's overall cost.

I believe the military has an important role in the FTS2000 program and must take an active part in working toward a integrated government telecommunications system. DoD, though not currently part of the FTS2000 program, must examine the possibilities of this system and participate in the development of policy on its utilization. National defense rests not only on how well the military uses the telecommunications means available to it but also on how well it can integrate with the rest of the federal government. Can national interests better be met through the military participating in the FTS2000 service offerings instead of developing a completely different system of their own? If so, what factors figure in making these decisions? If the military did participate, what impact would it have on the FTS2000 project? On federal communications as a whole? What are possible alternatives and options the military should consider to become part of the FTS2000?

This thesis does not attempt to present a detailed technical evaluation of the FTS2000 program but instead explore policy issues that have led to its inception and what role I see the military playing in this program. Chapters II and III study the decision process leading up to the FTS2000 and how the new policy will alter the way government handles its telecommunications business. Then, Chapter IV. examines the FTS2000 system itself to see what this program has to offer. Chapter V. explores a number of issues delaying the program so as

to uncover applicable lessons learned for future telecommunications programs. This is then followed by Chapter VI. which explores the problems the military have expressed with the FTS2000 and presents the reasons for the military's continued involvement in this program. Next, Chapter VII. proposes alternatives and options the military could consider in working with GSA in the FTS2000 program. Finally, Chapter VIII recommends policy initiatives for the government, derived from my analysis, with the goal of arriving at an integrated approach to government telecommunications policy.

This thesis is based on numerous government documents and interviews with decision makers in various government agencies involved in the program. Documents included GSA's directives and studies that lead to the *FTS2000* and *the Request for Proposal* (RFP), including applicable amendments. Also included in the study were General Accounting Office's (GAO) studies on the FTS2000 program and the effectiveness of GSA and Office of Management and Budget (OMB) in meeting the federal government's telecommunications needs. Furthermore, I researched applicable executive orders and public laws for an understanding of government's positions on issues such as telecommunications, competition, and National Security and *Emergency* Preparedness (NSEP). Once having studied the documents, I interviewed key people at GSA, Defense Communications Agency (DCA), GAO, the House Government Operations Committee, National Science Foundation (NSF) and the National Communications System (NCS). Finally, I followed weekly

accounts on the FTS2000 program in the media to determine the program's direction as it faced policy changes and political issues.

Technical information came from a number of books and papers on telephony, data and digital technologies, networking, packet switching, ISDN and ISO standards, and video conferencing.

Finally, I utilized the combined expertise of my thesis directors and professors along with my own experience as a military telecommunications officer to digest and integrate this information.

CHAPTER II

FTS, AUTOVON and AUTODIN

The federal government presently relies on the Federal Telecommunications System (FTS) for the majority of its voice and slow speed data traffic. The military relies on its own dedicated networks, the Automatic Voice Network (AUTOVON) and Automatic Digital Network (AUTODIN). All three were established in the 1960's to meet the growing telecommunications needs of the government. This chapter will concentrate on FTS with a brief introduction to AUTOVON and AUTODIN. However, all three networks are similar in purpose, design and problems they are now experiencing.

The FTS

The FTS was established in 1961 and put into operation on February 14, 1963, to meet three fundamental needs of the federal government: national security, cost savings and addition of enhanced services.[1] First, in the interest of national security, the FTS was built to guarantee the federal government a communications system to unify all agencies under all conditions, ranging from daily operations to national emergencies, including

nuclear war. This was in response to emergency preparedness actions developed during the Kennedy administration.[2]

A second reason was to cut growing government telecommunications costs. Before this time, each agency was required to seek its own telecommunications service. This was becoming extremely expensive as agencies within the same building were purchasing separate services. By integrating the different needs of each agency under one system, economy of scales could be achieved.

Finally, the government was seeking enhanced services which smaller agencies could not afford. Services such as audio conferencing, specialized attendant services and recorded message announcements were beyond the scope of most small agencies or remotely located offices. By concentrating all the requirements into one system, every agency could enjoy the services of the network for a reasonable cost. Consequently, the FTS was an effective solution to the governments needs of the 60's.

System

The FTS is a major telecommunications network. Consisting of an intercity backbone, it provides analog voice and slow speed data services to over 1,200 federal agencies. It spans the continental United States, Alaska, Hawaii, Puerto Rico and the U.S. Virgin Islands. The system handles over 1.5 billion minute calls per year at a cost of 400 million dollars a year, making it the largest private network in the world.[3] To get a better idea of its

size, the FTS system is equal to the next 17 largest private networks, including General Motors and General Electric, combined. Fifteen percent of the network handles data, making it also the largest private data network in the world.[4]

The network consists of 52 leased switches, transmission lines and station sets. Switching equipment includes private base exchanges (PBX) and CENTREX services.[5] AT&T owns most of the switching equipment and is responsible for most of the network's operation. This network is linked by 15,000 long distance trunks and about 35,000 access lines provided by seven vendors, ranging from MCI, Sprint and other regional long distance suppliers. The technology used ranges from satellite, microwave and land lines. The system is accessed by 1,655 local switchboards and 1.3 million telephone sets.[6]

FTS is a dedicated, fixed system of switches and trunks, leased for government use only. Usage costs are determined by mileage and number of terminations into the different switches. This is similar to the Bell Direct Distance Dialing (DDD) system, using an uniform dialing plan, direct station to station dialing, on/off net calling, automatic alternate routing and national conferencing.[7]

Originally, AT&T operated the system for the GSA, leaving the government with only an oversight role. Furthermore, due to the bulk of government traffic, the FTS enjoyed the special long distance tariff called TELPAK, an AT&T offering which made the network a cost effective solution to government communications needs up through the 1970's.[8] However, by the 1980's, major

challenges faced this once reliable and economical telecommunications network.

Problems

The FTS has served its purpose well but it is now facing serious problems. GSA has identified the following four as the most critical:[9]

-Inadequate service

-Degrading system quality as result of technical obsolescence

-Scarcity of good management information

-Rising system costs

Inadequate Service

The present FTS cannot provide the increasingly varied services needed by the government agencies it serves. The FTS is an analog voice network which can only handle low speed data transmissions through modems. Data transmission was not a concern in the original network design. Presently, digital transmission lines have been added in certain areas but constitute only 15% of the overall system. Therefore, the network cannot handle the higher speeds, larger bandwidths and digital formats required to process the enormous quantity of data now used in running the federal government. Moreover, these network weaknesses limit other value added services such as video conferencing, advanced networking features, imaging techniques,

etc. now in demand by federal agencies. Consequently, most agencies now look elsewhere for data services, increasing cost and loss of interoperability within the government.[10]

Degrading System Quality/ Equipment Obsolescence

Most of the FTS equipment is over 20 years old resulting in a drop in responsiveness and overcrowding as it copes with loads and requirements it was never designed to handle. The backbone switches are the most critical to the system and are the oldest part of the network. They are experiencing increasing technical difficulties, making them less reliable and more costly to operate. Additionally, they were designed in the era of analog technology, so they lack the necessary flexibility to handle the proliferating digital data traffic. Furthermore, they have limited capacity and hardwired routing schemes, so they are flooded with growing number of system users and heavily burdened by the resulting congestion across the network. All this cuts back on the systems responsiveness, aggravating the user while increasing their cost to use the network.[11]

The FTS network is fixed and inflexible to handle increasingly complex networking strategies. It was built in an era when the hardware (transmission lines and switching locations) defined the network. Today's networks use software to reconfigure and manage traffic flow patterns, routing traffic around congested areas to free up transmission media and use them more effectively. Unlike the software defined networks, the FTS relies on switches to handle whatever traffic comes there

way. Congestion is alleviated by buying more trunks entering or leaving a switch, a costly and wasteful procedure for a temporal problem. Furthermore, any changes or upgrades to a hardware network requires tremendous capital investments to replace major segments of equipment. Changes to software networks require only updating the software, not the equipment itself.[12]

Scarcity of Management Information

GSA is confronted with limited management information to make critical operational decisions on the FTS. As a hardware defined network, it lacks the real time status reporting found in software networks. This makes it extremely difficult to find and respond to problems in a timely manner. Consequently, GSA finds itself fighting brushfires without the needed information to act on the problem before they occur.[13]

A second major problem is the lack of accurate billing information. The present billing system was built in 1960 on now aged COBOL equipment. It is based on mileage and number of terminations onto the backbone. This method provides only limited management information for voice traffic users. The system is designed to simply add up total costs and divide this figure by number of calls. In today's competitive environment, users need accurate, up-to-date management information to track expenditures and compare alternatives to achieve the best cost savings. Moreover, this billing system fails to take into consideration data transmissions.[14] Digital data traffic, unlike analog voice transmissions, is measured by a different set of

parameters. Data usage is measured by duration and capacity used (speeds and bandwidth). Mileage and terminations have little relevance with how the user employs a data network.

Rising System Costs

The loss of the bulk tariff, TELPAK, as well as the increasing cost of operating the network have made FTS a costly service to the government. TELPAK, offered by AT&T, was a special rate offered to large, bulk users such as the government. This tariff made the original FTS a very cost effective solution for the government. GSA estimates that TELPAK saved the federal government over $1.25 billion during the 1970's.[15] The average call in 1980 was approximately 91 cents per call, a 15 cent increase over the 1970 rate of 76 cents while inflation had doubled the cost of most services. Unfortunately, it was too good a deal. MCI applied for the same rates to then resell services to commercial interests at lower costs. AT&T protested, denying MCI the tariff. MCI filed a suit with the Federal Communication Commission (FCC). The commission ruled in favor of MCI, stating TELPAK, as any other tariff, was available to the public at large.[16] AT&T countered by withdrawing the tariff in 1981. The cost per call rose 27% the first year and 29% the next. GSA estimates it could have risen as much as 34% the second year had they not taken an active role in aggressively competing most transmission services. However, this cost savings comes with increased GSA daily involvement for usage charges barely lower than that

offered by the increasingly competitive long distance telecommunications market.[17]

The government would need to make a major investment to upgrade the current FTS network. This effort would include updating/replacing existing equipment, introducing effective management information systems, installing software network management capabilities, etc. Unfortunately, since the FTS has such a widespread analog base, the investment to modify it would equal or exceed the cost of building a new network.

AUTOVON

The Automated Voice Network (AUTOVON) was established by the military in the mid 60's in similar fashion and purposes as the FTS. AUTOVON consists of two segments, a US (CONUS) and Canada network and a worldwide network. The CONUS segment consists of a AT&T leased network of 60 dedicated switches linked by 2- and 4-wire, analog trunks from the PSN. The network nodes consist of a mixture of AT&T #5 Crossbar and #1ESS, and Automatic Electric Company (AECo) electronic switches handling analog voice and slow speed data.[18]

Although similar to the FTS, the AUTOVON network has additional features to meet military requirements. Among these is the a system of precedences and priorities. There is a hierarchy of call precedences. If a call of higher precedence encounters busy trunks, it will preempt lower precedence calls, dropping them from the system. A second unique feature is the polygrid

architecture. Unlike the hierarchal structure of the PSN, all AUTOVON switches are linked to each other. This ensures survivability should an attack or system fault make inoperable one of the network nodes. Additionally, the AUTOVON switching facilities have more stringent hardening and security requirements to further ensure their survivability. Finally, AUTOVON is a dedicated network with interoperability to other military systems alone. Connectivity with the PSN is possible only through specialized interfaces, providing only limited interoperability.

AUTOVON suffers from the same ailments now facing the FTS. The switches are old, hard to maintain and expensive to operate. Built during an era of hardwired networks, it has become inflexible to handle it's increasing traffic load. To upgrade the network to handle software networking features and digital traffic would require a complete replacement of all switches. Furthermore, AUTOVON network lacks the necessary management information and network management systems to effectively evaluate and control its performance. Finally, it has become an extremely costly system to operate. Therefore, the military, as GSA with FTS, is faced with the need to replace the network.[19]

AUTODIN

The Automated Digital Network was established in the same timeframe as FTS and AUTOVON to provide the military with

message transmitting capabilities.[20] The CONUS AUTODIN is a CONTEL (originally Western Union) leased service consisting of a network of nine electronic switches arranged in a polygrid architecture similar to AUTOVON. The nodes consist of computerized switches (490L). These are presently being replaced by Northern Telecom DMS 100/200 switches under current upgrade programs. The network, originally analog, now operates in digital format at transmission rates up to 4800 baud. Its network accommodates both general service (GENSER) and Defense Special Security Communications System (DSSCS) traffic. As with AUTOVON, AUTODIN has an established set of precedences to ensure urgent messages manage to transverse the network when needed. The priorities are Routine, Priority, Immediate, Flash and Flash Override, with Routine being the lowest priority and Flash Override the highest.

The system operates on the principle of "store and forwarding" of message traffic. A message is transmitted to a switch, stored until it is received and corrected for errors, and then transmitted on to the next switch. This process can cause delays in the network at higher data speeds as switch capacity is tied up with half completed messages waiting error checking before retransmission.[21]

AUTODIN offers its users five basic modes of operation, depending on the terminals used or message traffic passed.[22] Mode I and V, the ones most used, offer full duplex transmissions with automatic error control and channel coordination, the first synchronous and the second asynchronous. Mode III offers

duplex, synchronous transmissions with one way serving for message transmission and the return for error control and channel coordination. The direction the message takes can be reversed based on the message. Mode II provides full duplex, asynchronous transmissions, uncontrolled except for precedence and special routing indicators. There is no positive message acknowledgement in Mode II. Finally, Mode IV is a uni-directional Mode II.

Again, as with FTS and AUTOVON, AUTODIN system is now undergoing major upgrades to help it cope with the higher data rates and transmission capacity. However, it lacks many of the important networking and management information tools that could improve its efficiency. Therefore, cost of operating and maintaining are becoming too high. Consequently, the military is now working on replacing it with digital, packet switching technology to meet military needs of the future.[23]

Conclusion

Both GSA and the military are faced with major problems with their networks. All three are barely meeting the current user need for voice or data traffic. Their architectures are inflexible, analog structures making newer, desired capabilities such as larger capacity, higher data speeds, digital technologies and value added services prohibitive. Updating the existing switches would be extremely costly and would not solve all the problems. Therefore, both GSA and the military are faced with

replacing FTS, AUTOVON and AUTODIN as their only cost effective solution.[24] The issue then is with what and how to replace the existing service with minimum impact on the users? Chapter III studies the decision process and the resulting strategy adopted for replacing the FTS.

NOTES-CHAPTER II.

1. US General Services Administration, Office of Information Resources Management; The Federal Telecommunications System (FTS) Intercity Program Changes in the 80's; February 1984; pp. 3-4

2. Establishment of the National Communications System ; Memorandum of August 21,1963; 3 CFR 1959-1963 comp., pp. 858-860

3. US General Services Administration, Office of Information Resources Management; Changes to Federal Telecommunications System (FTS) Intercity Services-Advanced Notification and Request for Comments; Federal Information Resources Management Regulation (FIRMR) Bulletin 29; 15 October 1985; p. 2

4. US General Services Administration, Office of Information Resources Management; Request for Proposals for Strategic Analysis (Cost Benefit Analysis) of Alternatives for the Replacement of the FTS Intercity Network; Section C, Statement of Work; August 1985; p. 3

5. CENTREX is a leased service offering by the Bell Telephone Co. It provides medium to large size customers with a dedicated network offering station-to-station dialing, on listed directory numbers, direct inward dialing, and station identification on outgoing calls. This service resembles that offered by a PBX but is handled from a Central Office switch. For more information see Engineering and Operations in the Bell System, Second Edition by AT&T Bell Laboratories, pp. 58-59, 67-70.

6. Request for Proposals for Strategic Analysis (Cost Benefit Analysis) of Alternatives for the Replacement of the FTS Intercity Network; Section C; p. 3

7. The Federal Telecommunications System (FTS) Intercity Program Changes in the 80's; p. 3

8. Ibid.; p. 4

9. From conversations with Mr. Walter Irving, Information Resources Management Services, General Services Administration and from the introduction documentation to the FTS2000, presented in session five of the meeting between the General Accounting Office and General Services Administration-July 21, 1987; Exhibit 7

10. Ibid.; Exhibit 5 and 6

11. Ibid.; Exhibit 5 and 6

12. B.R. Hurley, C.J. R. Seidl, W. F. Sewell; "A Survey of Dynamic Routing Methods for Circuit-Switching Traffic"; IEEE Communications Magazine; Vol. 25, No.9; September 1987; pp. 13-21

13. From conversations with Walter Irving, GSA and from the introduction documentation to the FTS2000, presented in session five of the meeting between the General Accounting Office and General Services Administration-July 21, 1987; Exhibit 5 and 6

14. Ibid.; Exhibit 5 and 6

15. FIRMR Bulletin 29; p. 6

16. Ibid.; p. 6-7

17. The Federal Telecommunications System (FTS) Intercity Program Changes in the 80's; pp. 6-7

18. From information in AT&T Bell Laboratories; Engineering and Operations in the Bell System; Second Edition; 1983; pp. 91, 399 and Integrated Long-Haul Communications; Student Text KEO 3000-124; 3395th Technical Training Group; Keesler AFB, MS; April 1978; pp.35-43

19. Christine Bonafield; "Defense Plans Would Create Billion-Dollar Carrier Contracts"; Communication Week; April 13, 1987; No. 139; pp. 1, 85

20. Extracted from conversations with Mr. Charles Letche, DCA AUTODIN Program Management Office and Defense

Communications Agency, DCA Code B670; AUTODIN System Functional Specification; January 1987.

21. For more information on "Store and Forward" or "Message Switching" techniques, see William Stallings; Data and Computer Communications; Macmillan Publishing Co.; New York, NY; 1985; pp. 194-197, 199-203

22. AUTODIN System Functional Specification; pp. 2-8 to 2-25

23. Bonafield; "Defense Plans Would Create Billion-Dollar Carrier Contracts"; Communications Week; No. 139; April 13,1987; pp. 1, 85

24. FIRMR Bulletin 29; pp. 1-2

CHAPTER III

DECISION PROCESS LEADING TO A NEW SYSTEM

GSA is faced with the need to replace the FTS with a system that not only meets the present needs of the federal government but can handle any future requirements arising over the next 10 to 15 years. This is a very difficult task in an age of tremendous telecommunications innovation and growth. Moreover, fiscal realities have changed considerably to those originally encountered in the 1960's. This chapter deals with GSA's decision process in finding the ideal replacement for the FTS.

Peter Keen, in his book Competing in Time [1], laid out a framework in which to develop telecommunications strategy in this era of change. He presents a threefold process: vision, policy and architecture. First, one must have a complete vision of the environment in which the system will operate and the community it will serve. From this vision arises a policy to use as a guideline in evaluating alternatives. Finally, one can formulates alternatives and then matches them against the policy to find the one that best fits the vision. This best alternative then becomes the architecture for the new system. This chapter follows this framework to study the decision process used in finding a replacement for the FTS.

Vision

Two main areas have the greatest impact on all future telecommunications acquisitions within the federal government: trends in the telecommunications and fiscal realities faced by the government. Each needs to be studied in-depth to get a clear vision of the government's future telecommunications needs.

Trends in Telecommunications

The telecommunications field is highly dynamic. With the advent of new technologies, new and varied services are now available for the consumer at extremely competitive prices, especially in the area of long distance communications. This explosion in telecommunications services is in part due to three reasons: changing technology, evolving user needs and a volatile marketplace. Each impacts the other and have made the telecommunications business one of the fastest growing segments of the world economy.

Changing Technology. The marriage of computers and telecommunications has caused an explosion in technological innovation. Software has replaced hardware as the driving force of change. Computer controlled switching and terminal equipment allow the telecommunications manager to alter the structure of his network through minor software changes. This hasproduced accurate, real time network management information, improving efficiency and cutting costs. It has also led to the commonality in

hardware. Equipment is now mass produced and interchangeable with that of other vendors, cutting back on manufacturing costs. Network upgrades no longer require a complete equipment change. Instead, the existing equipment is reprogrammed with new software without loss of service or need for major capital investment. This has revolutionized telecommunications management strategies.[2]

A second major change in technology is the move towards digital techniques. Digital techniques encode signals into strings of ones and zeros, simplifying their transmission while improving the overall transmission quality over that of analog techniques. This makes it possible to transmit more information at higher speeds and requiring larger capacity than on an analog system. Furthermore, with information already in digital format, encryption is easier and cheaper to implement. Finally, digital accommodates the newer services and technologies now being developed throughout the industry.[3] Integrated Services Digital Networks (ISDN) is one such effort.

ISDN is a set of standards for integration of voice, data and video services onto transparent transmission medias through digital techniques. This standardization effort is driven by the International Telecommunications Union in an effort to integrate the world telecommunications community. The US is a major participant in this effort and strongly endorses its implementation. Most new telecommunications switching and terminal equipment advertise provisions for ISDN compatibility.

This standardization effort could further revolutionize an already dynamic telecommunications environment.[4]

A further change in data transmission technology has been the advent of packet switching. Basically, packet switching takes the information to be transmitted, breaks it into small fragments or packets, and sends these across the network. The receiver reassembles the information from these packets and passes it onto the user. Since the packets are designed to occupy only a fraction of the system's capacity, many users can use the same media at the same time. This especially useful for interactive information traffic, such as used with the personal (PC) and home computers. Interactive systems transmit short bursts of information spaced among long periods of inactivity. The PC user perceives their system is operating continuously but to a telecommunications network operating in real time, this type of traffic can tie up a line for extended periods of time with relatively little activity. Packet switching, on the other hand, allows the transmission media to be shared by many users "taking turns" sending their packets. This frees up transmission assets, cutting costs and increasing system effectiveness.[5]

The transmission media itself has made great technological advances. Fiber optics, digital microwave, improved satellite transmission techniques and T-carrier systems have produced tremendous bandwidths and high transmission speeds. This expanded capability provides the network with qualitative and quantitative improvements over the older analog wire and radio techniques at a fraction of the cost.[6]

Couple all the above changes into the enormous and richly connected public switched network (PSN) serving the US makes for tremendous opportunities for the telecommunications industry. The PSN represents an investment of about 250 billion dollars, considered by many as the US's greatest information asset. It provides selective, two-way telecommunications for voice traffic as its primary service objective, and data and video traffic to a lesser extent, linking business, industry, government and residential users through 19,000 telecommunications centers nationwide. This service is provided by a cohesive set of networks (over 1400 local exchange carriers alone) through a well defined body of standard interfaces.[7] These nodes are linked by more than 1 billion miles of transmission paths, including 6 million trunks and as many special services circuits; and about 100 million loops connecting customers to the central offices.[8] Key to its success is a universal numbering plan, providing each user a unique identification, and the standardized interfaces that interconnect the many local and long-distance networks into on integrated system. These two factors make the PSN a national asset, unique in size and functionality in the world.[9]

Finally, the changes in automated data processing (ADP) has given rise to the smart terminal and local area networks (LAN). These terminals are no longer "dumb" recipients of information but actual manipulators of data which have slowly replaced the larger main frame computers as the point of actual data processing. These terminals in turn require transmission links to other terminals as well as to the larger data bases. This has given

rise to LANs which connect the users together. LANs link users not only in their offices but across agency lines, decentralizing a once centralized data processing community within the government and business.[10]

To meet the proliferation of different terminal and network technologies, the International Standards Organization (ISO) developed the Open System Interconnect (OSI) seven layer model. This standardization effort will help in interconnecting the diverse LANs and Wide Area Networks (WAN) to achieve interoperability. Any new telecommunications system will need to integrate this standard into its network to cope with the diversity of equipment and protocols available in the marketplace.[11]

Evolving User Needs. Today's user requires far more information to handle the growing complexities of government business. Telecommunications is the key to linking agencies to themselves, to other segments of government and to the information's sources outside of the government. The telecommunications system must be able to handle each required service to best serve its user community.

The growth in automated data processing (ADP) has brought many changes to the way government handles its daily business transactions.[12] Among the changes is a shift to decentralizing agencies through distributed processing and personal computers in the workplace to improve efficiency. The main frame computers are becoming data base repositories, with most of the

data processing occurring in the workplace on mini or microcomputers.

This shift brings a new set of problems to the telecommunications system. First, greater volumes of traffic are interactiveor bursty in nature. The PC user only transmits short burst of information space over long pauses. This is very inefficient assuming the system is on a dedicated line. Then, there is a growing need to link these different interactive microcomputers among offices, and these offices to other agencies or to the main frame computers. LANs now carry this decentralized data traffic between user communities. These LANs, however, tie up transmission assets originally intended for voice traffic alone. Consequently, government now requires transmission systems with greater capacity and higher speeds, in digital format, to handle the growing diversity in data traffic loads.[13]

Another major change in the users requirements is the need for value added services over their telecommunications system.[14] These services range from call management functions to some intelligence in routing and tracking traffic. Call management functions include use of features such as call forwarding, call queuing, etc. to improve the efficiency in handling of message traffic. Intelligence provides call status, prerecorded messages, software driven network routing, etc. to better manipulate the information being sent or received. These services are growing more diverse as the technology evolves and future

telecommunications systems must be flexible enough to accommodate them.

A recent innovation of growing interest to the user is video and imaging services. Video services include conferencing and broadcasting. Though previously prohibitive in cost, new techniques in signal compression have reduced the transmission capacity required to transmit video without great loss in clarity. This translates into conferencing ability at affordable costs. Imaging services include facsimile and graphics (such as used in computer aided design). With decentralization, both video and imaging service will become more important to link physically separated offices through their telecommunications system. Therefore, future networks must be capable of offering these services to meet organizational needs.[15]

Finally, in an era of improved technology comes greater, it becomes harder to ensure adequate security and privacy. As the government accumulates greater amounts of information on the private citizens of this country in its data bases, security and privacy become essential. Any new telecommunications system must incorporate the necessary security measures to protect not only the government's operation but ensure each citizens privacy.[16]

Volatile Marketplace. Major changes have occurred in the telecommunications industry over the last decade, creating an extremely competitive and changing marketplace. Unlike the monopolistic environment of the 1970's, today there is a

proliferation of providers and service offerings. Many factors have given rise to this phenomenon, among which are the deregulation of the industry and the divestiture of the Bell Telephone Co. These events coupled with the innovations in technology have opened up diverse new fields in telecommunications.

The events leading up to the deregulation of the industry with the eventual breakup of the Bell system (divestiture) have opened new competition in a once regulated market.[17] A major impact of deregulation has been the opening of the long distance market to other commercial carriers, such as MCI and Sprint Communications. Coupled with technological innovations, deregulation also brought about value added services. This has, in turn, given rise to numerous *telecommunications* firms specializing in providing the value added services.

A major side effect of deregulation is the loss of one-stop services.[18] Before the breakup of the Bell system, Bell engineers handled all network user requests. Today, there is no one entity with total knowledge on end-to-end services. This decentralization has led to uncertainty among users, making the telecommunications managers job more complex. It has also given rise to another new market for system integrators and consultants to tie together the different fragments into functional end-to-end networks.

Finally, as result of the efficiency of new media, especially fiber optics, there is now a glut of transmission capacity. This is

driving down the cost of transmission and translating into savings for the network users.[19]

Fiscal Realities

GSA is not only faced with the dynamics of the telecommunications industry but must consider the changing fiscal realities facing the government. Balanced budgets, competition, and national security issues will all have an impact when planning any new telecommunications system.

Balanced budget legislation under the Gramm-Rudman-Hollings Balanced Budget Act, introduced in 1985 and revised in 1987,[20] epitomizes the general sentiment in government and the public that federal spending must be cut back . These cutbacks will limit capital available for the acquisition and operations of major systems. This will make the government seriously consider sinking limited funds into dedicated, government-owned facilities. Furthermore, projects that survive one year may suffer the next. This uncertainty in funding will make only the most efficient and/or self supporting government projects viable.

Competition has become a major part in government acquisition. Congressional pressure in legislation such as the Paperwork Reduction Act of 1980[21] is pushing competition to eliminate waste and abuse in government procurement process. All contracts must be competed to ensure the government gets the best deal for its money. President Reagan's push for privatization of public services where ever possible has further decreased the number of government owned and dedicated facilities. Office of

Management and Budget (OMB) Circular A-76 best defines the President's policy as, "...the government [should] rely on commercial sources to supply products and services to meet government needs whenever possible."[22]

A third reality facing the government is an increasingly difficult task of attracting and retaining qualified technical people. This has become extremely problematic in technical areas such as telecommunications and information processing. Unfortunately for the government, this is an area that now needs greater expertise as the industry becomes more decentralized and technically sophisticated. Future system planning will have to deal with this reality, seeking labor saving alternatives to economize technical expertise.[23]

A positive side to the personnel issue is the government does count with a very qualified cadre of contract administrators. These specialist have experience in diverse areas of contract development and management. This resource should be exploited in lieu of the loss of the technical expertise.[24]

Interoperability and standardization are key to the successful operation of the federal government. The Paperwork Reduction Act of 1980 calls for increased need to share or combine agency resources to attain interoperability while reducing redundancy and waste. As the federal government grows in complexity and size, interoperability between agencies become essential to access different data bases, improve coordination, and ensure the effective utilization of government

assets by all. Consequently, standardization of interfaces and network functions becomes imperative.

Interoperability and standardization are also extremely important to the success of the National Security and Emergency Preparedness (NSEP) program.[25] NSEP program provides the means for the government to resolve emergency situations the nation may encounter. Key to NSEP is a survivable telecommunications system able to operate under all conditions. This system must incorporate hardness, redundancy, mobility, connectivity, interoperability, restorability and security. The FTS is an integral part of the NSEP network. Its replacement will need to not only fulfill FTS's part in the NSEP program, but also anticipate future requirements.

The government's size as a consumer group gives it significant leverage in negotiating contracts.[26] The FTS is presently the largest private telecommunications network in the world. Its operating costs exceed 400 million dollars per year. Moreover, the FTS is a nationwide network. Size and scope of a replacement would be a prized contract to any vendor within the telecommunications industry. This fact offers the government tremendous leverage in negotiating such a contract. If all government agencies could come together under one network, the government could dictate its conditions with the certainty of achieving them.

Finally, the transition process from the FTS to an alternate system will be a major undertaking.[27] As mentioned previously, over 1.3 million government subscribers rely on the system for

their daily long distance requirements. Any transition will need to occur with minimum disruption to this service. Extensive delays resulting from a new system cutover would translate into the losses in the millions of dollars and hours of key government resources.

Policy

Having defined the environment under which the new government telecommunications system would operate, GSA formulated policy to select an effective system architecture. These policy objectives are as follow:[28]

-The existing FTS network must be replaced.

-The new network must provide state-of-the-art, upgradable and integrated services. Its architecture must accommodate the government's present and future telecommunications requirements up through the year 2000. Furthermore, the government is committed to integrated services and any system chosen will have to migrate towards integration.

-Competition will be used whenever possible to purchase telecommunications services at the best price.

-Private enterprise has the best understanding on the future direction of the telecommunications industry, government does not. Therefore, government will purchase services only, expending no capital investments, and let industry find the best way to provide them. Furthermore, the network should capitalize

on the existing public switching network to effectively use existing national resources.

-Government will capitalize on its strength in contract management changing its role from facilities management to service oversight, relying on industry for technical expertise.

-Government will concentrate their telecommunications requirements into one effort to effectively use its leverage as a major consumer block.

-Transition to the new system must be transparent to the user agencies.

Architecture

Several strategies were analyzed using the previously stated policy objectives as a decision framework. After study and comments from different government agencies, GSA devised four final strategies. Under contract by GSA, Kalba Bowen Associates, Inc., a research organization, studied these alternatives in-depth. A summary of their study as well as GSA's final assessment are listed below:[29]

Decentralized Procurement by each agency of their own networks

Under this first strategy, each agency would be on their own to purchase inter and intracity services they require. GSA would serve only as as system integrator to encure standarized procedures and technical specifications are implemented in each agencies network.

The advantages to this strategy are:

-Best approach to fostering competition, involving the most vendors in the procurement process.

-The agencies would perceive a cost savings as they would now manage their own networks.

-This option provides for the least risk with only short term commitments for individual network of the other three options.

-Each agency would have autonomy over their communications systems.

The disadvantages to this approach were:

-This option would create the most management and coordination problems

-Most labor intensive as each agency would need to have a complete staff of technicians and contract administrators overseeing their entire networks. This would lead to considerable redundancy and waste of valuable human resources.

-Inflexible to change or upgrades on a nationwide scale.

-Loss of new service options and economies of scale compared to a larger, unified network approach. Agencies would have access to only those new services they could afford.

-Standardization would be impossibel for an overall government system. Standards would have to be implemented within each agency's network, leading to delays and incompatibility among vendors, which could eventually result in the loss of connectivity between networks.

-Loss of cost visibility and control for planning and management purposes.

-Loss of a interoperable, nationwide network to meet NSEP requirements.

-Integration of services would be nearly impossible across a myriad of different vendors' networks.

GSA would centrally procure an intercity network to tie together agency owned intracity networks.

Under this approach, GSA would manage an intercity network, much like the long distance provider, leaving the intracity networks to each agency. Each agency would procure and manage their individual networks by guidelines established by Office of Management and Budget (OMB) and GSA. Each of the networks, inter and intracity, would be competed among numerous vendors.

The advantages to this strategy are:

-The agencies would perceive a cost savings as they would now manage their own networks

-There is relatively little risk with only short term commitments for individual networks, instead of the greater risks associated with longer committments that come with the larger networks.

-Each agency would have autonomy over their communications systems.

-The increased opportunity for competition would give more vendors an opportunity to participate in the program.

The disadvantages to this strategy are:

-Significant management and coordination problems arising over the entire network.

-Labor intensive as each agency as well as GSA would need to have technicians and contract administrators overseeing each segment of the network

-Loss of flexibility to change or upgrade the network since no one agency has control over the entire system.

-Loss of new service option and cost savings compared to a larger, unified network. Agencies would have access to only those new services they could afford.

-Difficulties in standardizing the overall system. Standards would have to be implemented by each agencies system, leading to delays and possible loss of connectivity between networks.

-Integration of services would only be achievable within the intercity network.

Telecommunications services through a single system provided by a single vendor.

Under this strategy, GSA would contract with one vendor who would provide all services and network management. GSA would assume the role of contract oversight. The system would be designed in such a way that should the contractor fail to provide adequate services, GSA could rebid the contract with minimum impact on the networks operation.

The advantages to this strategy are:

-Cost savings resulting from competition for the original contract and then, should contractor fail, the flexibility to rebid the contract.

-Provides for enhanced capabilities and expansion, due its size and central control by GSA. This would not be possible in smaller, agency owned and controlled systems.

-The network would be controllable from a centralized point over one contract, simplifying contract oversight.

-GSA would realize considerable labor savings in that one contracto has responsibility for integrating and operating the network, not the government.

-Requires limited and centralized technical expertise at GSA, freeing up technicians at agency level as well as at GSA.

-Eases steps toward integration of services since changes need only go through one contractor to be implemented networkwide.

The disadvantages with this strategy are:

-GSA would still need to maintain an extensive oversight capability to ensure the contractor is abiding by the terms of the contract.

-Possible legal and jurisdictional challenges from vendors losing the bid. The losing bidders would find a contract this size worth contesting for. Should this fail, the winner could then be challenged on grounds of attaining unfair competitive advantage through control of this end-to-end national network. This goes against the spirit of deregulation, a major legal precedent set by the government in the telecommunications industry.

Purchase telecommunications services through a single system provided by multiple vendors and centrally managed by GSA.

The network would be divided among the vendors at the start by some prearranged percentage. During the contracts life, as new requirements arise, the vendor providing the best and lowest costing service would get the new business. GSA would assume the role of system integrator, ensuring the interoperability and integration of the network.

The advantages to this strategy are:

-Cost savings through competition among the different vendors. This would prevent "lock in" to one contract as experienced with the FTS and AT&T.

-Flexibility in providing options should one contractor fail to meet contract obligations. Should this occur, the other providers could absorb this load without major impact on the network.

-Requires limited and centralized technical expertise within GSA instead of spread throughout the different government agencies.

-Provides for enhanced capabilities and expansion, due to its size and central control by GSA. This would not be possible in smaller, agency owned and controlled systems.

The disadvantages to this strategy are:

-Labor intensive for GSA in tracking the activities of many vendors.

-Difficult to procure and assemble an integrated network in a multivendor environment. Furthermore, how to split up the network equitably without losing system integrity.

-Significant management and coordination problems for GSA in maintaining the network integrated on a daily basis, requiring an extensive oversight capability.

-Integration of services would be difficult to achieve as changes and upgrades must be coordinated and approved by all vendors before they could be implemented.

Alternative Selected.

Kalba Bowen Inc.'s final cost summary, after carefully studying factors affecting the FTS2000 growth projections over a 10 year period are summarized in Table 3-1. Key factors considered were cost, risks and benefits achieved by both the government and the contractor.[30] Even though a core network would appear the lowest cost to the government, by including the 9.6 Kbps traffic omitted in these calculations, it would lose out to the single or multivendor provider of a single network. Consequently, Kalba Bowen Inc. concluded that either the single vendor and multivendors providing a single, integrated network would tie for best alternative.[31]

The strategy that best fit GSA's desired architecture was the third option, procure telecommunications services through a single system provided by a single vendor. GSA favored this approach over the multivendor approach for it simplifying governments role in managing a network of this size through

one-stop service with a single system integrator. This would also make it the easiest option to move toward integrated services due to it requiring the least effort.[32] A service oversight center would be established to manage the system and report to GSA. GSA would then sell these services to participating agencies on a usage basis. This became the favored architecture for the FTS2000.[33]

COMPARISON OF NET PRESENT WORTH VALUE OF COST FOR THE FOUR ALTERNATIVES TO REPLACE THE FTS

Alternative	Net Present Value of Cost, 1987-1996	
	Upper Quartile	Median
Independent Agency	$3.51 B	$3.19 B
Acquisition GSA Intercity Backbone	$3.21 B	$2.89 B
Single Vendor/Service	$3.35 B	$3.02 B
Multiple vendor/Services	$3.35 B	$3.01 B

Table 3-1

Source: Kalba Bowen Associates and Economics & Technology, Inc.; Cost/Benefit Analysis of Alternatives for the Replacemnt of the Federal Telecommunications System Intercity Network; Volume I, "Executive Summary"; GSA Solicitation No. KET-MS-85-12; May 30, 1986; p. 19

NOTES-CHAPTER III

1. Peter G. W. Keen; Competing in Time, Using Telecommunications for Competing Advantage; Ballinger Publishing Co.; Cambridge MA; 1986

2. B. R. Hurley and C. J. R.Seidl; "A Survey of Dynamic Routing Methods for Circuit-Switching Traffic"; IEEE Communications Magazine; Vol 25, No. 9; September 1987; pp. 13-21

3. John C. Bellamy in his book Digital Telephony; A Willey-Interscience Publication; New York; 1982; pp. 64-81, list nine technical advantages of digital communications networks. These are:

-Ease of encryption
-Ease of signaling
-Ease of multiplexing
-Use of modern technology
-Operability at low signal-to-noise/interference ratios
-Signal regeneration
-Accommodation of other services
-Performance monitorability

4. For information on ISDN, see evolution and standardization process in Dorothy Cerni's Standards in Process: Foundations and Profiles of ISDN and OSI Studies; NTIA Report 84-170; Dec 1984; pp. 155-163. For technical information, see William Stallings' Data and Computer Communications; Macmillan Publishing Co.; New York, NY; 1985; pp. 537-556

5. Stallings; pp. 197-203 and Bellamy; pp. 367-369

6. Stallings; pp. 45-60

7. Board on Telecommunications-Computer Applications, National Research Council; Nationwide Emergency Telecommunications Service for National Security Telecommunications-Interim Report to the National Communications System; Washington DC; August 1987; p. 16

8. D. M. Cerni; Standards in Process: Foundations and Profiles of ISDN and OSI Studies; NTIA Report 84-170; December 1984; p. 45

9. Nationwide Emergency Telecommunications Service for National Security Telecommunications-Interim Report to the National Communications System; pp.15-20

10. Andrew Tanenbaum; Computer Networks; Prentice Hall, Inc.; Englewood Cliffs, NJ; 1981

11. Cerni; pp. 171-190

12. US General Services Administration, Office of Information Resources Management; The Telecommunications Program Plan of the General Services Administration; August 1985; p. 7

13. Ibid.; pp. 7-8

14. Ibid.; p. 7

15. Ibid.; p. 7

16. Ibid.; p. 8

17. US General Services Adminstration; Changes to Federal Telecommunications System (FTS) Intercity Services-Advanced Notification and Request for Comments; Federal Information Resources Management Regulation (FIRMR) Bulletin 29; October 15, 1985; pp. 4-7

18. AT&T Bell Laboratories; Engineering and Operations in the Bell System; Second Edition; 1983; p. 34

19. The race is on between telecommunications vendors to become the first all fiber network. Consequently, there is a glut of capacity which is driving down prices. This is explained in Karen Gullo's article "Optics Net Wars"; Datamation; Vol. 31, No. 18; September 15, 1985; pp.48, 54, 59. The race to implement fiber in the local loop and its implications are described in Leonard Antelman, Robert Ristelheuber, Robert Vinton, and Stuart Zipper's article, "Fiber Optics-The Last Mile"; Electronic News; Vol. 32, No. 1629; November 24, 1986; pp. 30-31

20. Balanced Budget and Emergency Deficit Control Act of 1985; Public Law 99-177; 1985 and amended by Public Debt Limit Increase; Deficit Reduction Procedures; Budget Process Reform; Public Law 100-119 (HJ Res 324); September 29, 1987 and signed into law by the President on October 5, 1987

21. Paperwork Reduction Act of 1980; 44 U.S.C. 35, Public Law 96-511, 94 Stat 2812

22. Office of Management and Budget Circular A-76 (Revised); Performance of Commercial Activities; August 4, 1983

23. From conversations with Mr. Walter Irving, GSA and extracted from Session Five of hearings between with the General Services Administration and General Accounting Office covering the introduction FTS2000 RFP on July 21, 1987; Exhibit 12 and 13

24. Ibid.; Exhibit 12 and 13

25. Executive Order 12472; Assignment of National Security and Emergency Preparedness Functions; April 3, 1984

26. From conversations with Mr. Walter Irving, GSA and extracted from Session Five of hearings between with the General Services Administration and General Accounting Office covering the introduction FTS2000 RFP on July 21, 1987; Exhibit 13 and 14

27. US General Services Administration; Changes to Federal Telecommunications System (FTS) Intercity Services-Advanced Notification and Request for Comments; Federal Information Resources Management Regulation (FIRMR) Bulletin 29; 15 October 1985; pp. 4-6

28. Policy objectives as summarized from The Telecommunications Program Plan of the General Services Administration (August 1985); Session Five of hearings between GSA and GAO, Exhibit 14-16; and conversations with Mr. Walter Irving, GSA

29. Kalba Bowen Associates and Economics & Technology, Inc.; Cost/Benefit Analysis of Alternatives for the Replacemnt of the Federal Telecommunications System Intercity Network; Volume

III: "Benefit/Cost Model"; GSA Solicitation No. KET-MS-85-12; May 30, 1986

30. Ibid.; Volume I: "Executive Summary"; p. 19

31. Ibid.; pp. 19-23

32. From conversations with Mr. Walter Irving, Information Resources Management Services, General Services Administration

33. Conversation with GSA since writing of this thesis indicate that the multivendor approach, not the single vendor originally selected, will be choosen by the government. This comes from pressure from both the House Government Operations and Senate Government Affairs Committees. (See Chapter V for more details about the political issues)

CHAPTER IV.

FTS2000, A SYSTEM PERSPECTIVE

What does the FTS2000 offer the government? This chapter summarizes key aspects of the Request for Proposal to better understand the FTS2000.[1] This chapter does not attempt to delve in contractual and technical details but instead give a brief summary of the system.

Contract Terms

The FTS2000 is a fixed service contract. The winning bidder will provide all the necessary facilities, switching and transmission equipment, personnel and resources to complete the network. The government will then purchase services from that network. Even though the contract is for a ten year period, the contractor is only guaranteed usage of switched voice services for four years, a total of 450 million dollars out of the estimated 4 billion dollars the total contract is worth. Furthermore, the contract will be reviewed at the four, seven and ten year points to ensure the government is getting the service it needs at the best price. Should the government find at these reviews that the contractor is failing to meet the terms of the contract, then GSA

can terminate the contract without further obligation but the 450 million dollar guaranteed for switched voice services.[2]

The contractor will provide switched data, video,packet switching, integrated/digital and dedicated services as the users require. Even though every participating agency will have switched voice service, they are not obligated to use any other service. All services except integration are due in 12 months of contract award. No specific time frame is set for integration, just sometime during the life of the contract.[3]

The contract is fixed price. The price is set from the start of the contract. It can be adjusted downward to compensate for improved services or to make the FTS2000 service offering more competitive compared with the local commercial providers. However, *the price cannot be increased* except during formal contract reviews. Moreover, the cost of services must be consistent with the commercial rates charged in the specific area served. For example, the FTS2000 contractor cannot charge more for data services in Alaska than the price charged by the local commercial data providers.[4]

Federal agency participation in the FTS2000 program is voluntary. Initial participation calls for a four year commitment to ensure the contractor a minimum usage level. Nevertheless, should any participant find similar yet cheaper service through commercial means, it can drop out of the FTS2000 program without further sanctions. This puts additional pressure on the FTS2000 provider to ensure their services are competitive so as to keep and increase its government clientele on the network.[5]

Finally, the FTS2000 network must interface with other networks and contractors serving the federal government. These include the current FTS, other government networks and commercial systems. Other government networks include GSA's telecommunications programs such as the Washington Interagency Telecommunications System (WITS), the Aggregated Switch Procurement (ASP), and agency PBX buys.
This category also includes military networks such as AUTOVON and Defense Switching Network (DSN), NCS's National Emergency Telecommunications System (NETS), as well as other agency networks. Commercial networks include the public switching network and the numerous system providers in this domain. The FTS2000 must be fully compatible with these networks, working closely with the different contractors and government agencies to ensure interoperability.[6]

System Description

The FTS2000 system offers services to the participating agencies, leaving network management and operations up to the system provider. The user interfaces the network at service delivery points (SDP), choosing from among six telecommunications service offerings to meet their unique requirements. The prime contractor does the rest.
The system can thus be divided into SDPs, telecommunications services, and network management services.

Service Delivery Points (SDP)

The RFP defines SDPs as the combined physical, electrical, and service interface between FTS2000 and government premise equipment, off-premise switching and transmission equipment and other services (such as those provided by Centrex and telephone central offices).[7] This is the point where the government's equipment links with the network to get the desired services. In most cases, the SDP will be located at the trunk side of a government owned or leased switch (primary SDPs). However, as ISDN becomes available, there will be an increasing need to link terminal equipment, such as data terminals, host computers and digital telephones, directly to the network (secondary SDPs). Consequently, these interfaces are key to the user on the type of and access to services desired.

The primary SDP points are defined as the FCC telecommunication point for interconnection of local exchange carrier facilities to premise equipment. In other words, this is the point where the user equipment, usually a switching system, would interface with the commercially provided common carrier line or trunk. These interfaces vary by the way each agency handles its telecommunications requirements. For larger agencies with government owned PBX in a government owned building, the interface is at the building itself and to the trunk side of the switch. For agencies leasing transmission or switching equipment, the SDP would interface at the trunk side of the switch and the user would access it through the leased switch. Finally,

for smaller agencies without the need for dedicated switching equipment and who employ services offered through the common carriers such as CENTREX or a Central Office (CO)
provided services, the interface is at the CO itself.
Again, the user access the network through the switch.

There are occasions when a secondary SDP is required. This would involve a direct network interface to terminal equipment beyond the primary SDP. The need for such interfaces would arise in the case of CENTREX services and with ISDN connections. In the first case, the user would need to interface a terminal device, such as a host computer, directly to the network through a CENTREX system. The prime contractor would provide a trunk to the CENTREX switch and a virtual connection from there to the host computer, making it appear as a direct line to the network. In the second case, the prime contractor will need to supply ISDN services to terminal equipment beyond the agency's switch. To do this, the prime contractor will provide the interface adaptor to connect the user's equipment to the network, transversing the PBX.

Telecommunications Services

System user will have six service offerings to choose from to meet their voice, data and video requirements.[8] All system subscribers will automatically get switched voice access. From there, the user will need to specify which other type, if any, of services offered they wish to employ. The following lists the six telecommunications services including a short description of what

they offer, the types of user equipment served, and special features and relevant technical parameters they provide:

Switched Voice. This offers users voice and slow speed data services in analog format. The using agency can access this service either through the trunk side of a switching system (PBX, CENTREX or Central Office) or direct through the appropriate SDP. This service will serve a number of different user equipment types, including (see Figure 4-1):

-Single line sets

-Multi line key telephone systems

-PBXs

-CENTREX and/or Central Offices with feature group D (For smaller agencies without need for a PBX)

-CCITT Group I, II and III facsimil equipment

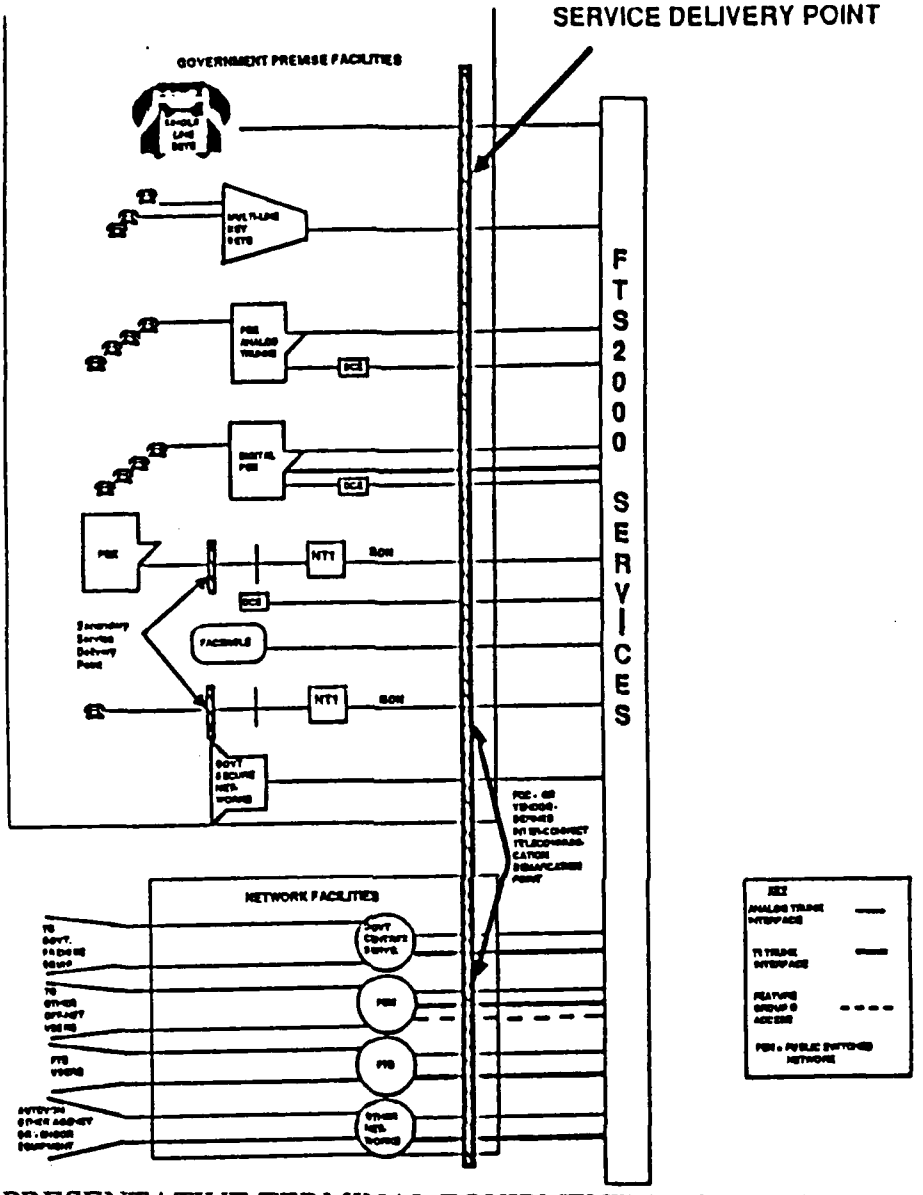
-T-1 digital terminating equipment

-Secure voice and data equipment

-Interface to other networks such as AUTOVON and DSN

Switched Voice services offers the user a number of features. These features include:

-On-Off net and Off-On net capabilities. This feature allows the user to access a called party either from a station on or off the FTS2000 network to another off or on the network. The system will automatically make the necessary number translations to complete the call.



REPRESENTATIVE TERMINAL EQUIPMENT AT SERVICE DELIVERY POINT FOR SWITCHED VOICE SERVICES

Figure 4-1

Source: General Services Administration, Office of Information Resources Management; FTS2000 Services, A Request for Proposals to Replace the Federal Telecommunications System; Amendment 1; March 1987; p. C-34

-Agency-Recorded Message Announcements. This allows agencies to place recorded announcements on the network, accessible from on or off network locations.

-Attendant Services. Call attendants or operators providing support services for the system user such as call completion, setting up audio conferences, verifying authorization codes, etc.

-Authorization Services. Each user is given unique authorization codes for network calling identification and class of service required.

-Call Screening. This set of features specifies the class of service assigned to a user, station or trunk. Utilizing the authorization code, calls can be completed or denied, depending on the class of service assigned to the particular user, station and trunk groups used.

-Network Audio Conferencing. This would include on-net, off-net and virtual on-net stations. Conferences can vary from 12 to 24 conferees to be connected simultaneously through either a preset or one time setup. This can be handled by the user or through an attendant.

-Inward Station Access. This is equivalent to the toll free or unit free services offered by the commercial common carriers in their 800 services. Off-net callers can be connected to predesignated FTS2000 stations by dialing a specified directory number. This feature would be most useful for agencies wishing to setup public information systems.

-Inward Selected Access. Gives caller a series of codes to use in selecting extra services or features once a station number is reached. This is accomplished through a prerecorded announcement specifying additional DTMF keyed codes.

Performance Parameters include:

-Utilize a 7-digit numbering plan

-Supports data rates up to 4.8 Kbps

-Bit error rates of 10-5 at 4.8 Kbps over 5 minute average using a CCITT V.32 Modem.

-Net average network busy hour blockage of 7% in busiest month.

-Interface specifications for analog and T-1 carrier systems (PBX, Centrex and Central Office offerings).

Switched Data. This provides the user with synchronous, full duplex, digital, circuit-switched, and high speed data services. User equipment to interface with this service would include:

-Workstations

-Host computers

-Personal computer

-Terminals

-Communicating office support equipment such as facsimil and data base systems

This service would offer the feature of authorization codes to identify user terminal device or application program. The FTS2000 system could then use this for call screening.

Unique parameters offered by this service are:

-System to support data rates up to 56/64 Kbps (when clear channel available)

-Utilize same 7-digit numbering plan as in switched voice service

-System will provide network derived clocking to data terminal equipment

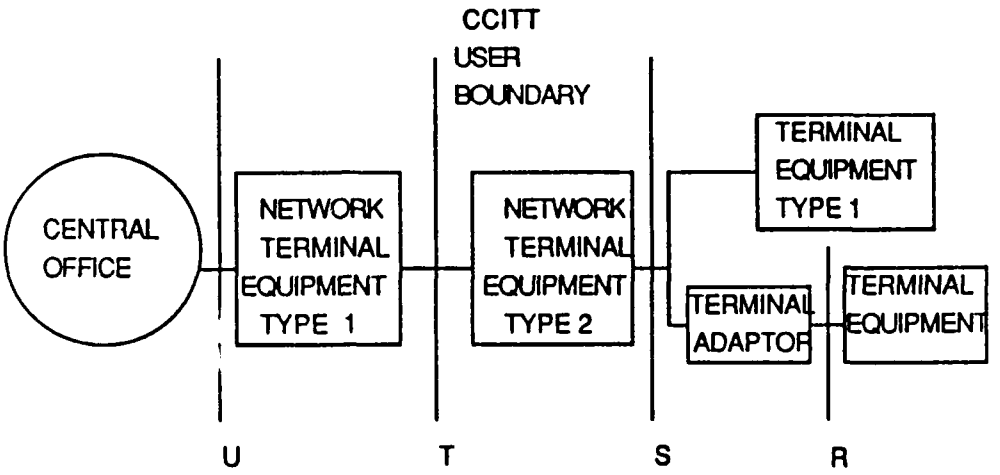
-Capability to interface network direct or through a digital PBX

-Point to point bit error rate of 10-6 either over a 24 hour period during initial acceptance or over a 15 minute period after service restoration

-Absolute propagation delay of 600 milliseconds from SDP-to-SDP.

-Net average network busy hour blockage of 7% in busiest month.

Switched Digital/Integrated Service. Provides users with integrated voice, data, image and video services in a digital format. This would be done following two digital standard formats, Integrated Services Digital Network (ISDN) and T-1 Carrier. System parameters and equipment interfaces with this service would depend on the format followed. ISDN standards are described in CCITT I and Q series for switched digital; integrated service. It relies on signaling system number #7. User equipment interfacing an ISDN network fall into three categories (see Figure 4-2).



ISDN REFERENCE POINTS

Figure 4-2

Source: "Recommendation I.4111, "ISDN User-Network Interfaces- Reference Configurations"; CCITT Red Book Volume III, Fascicle III.5, Integrated Services Digital Network (ISDN); Recommendations of the Series I; VIIIth Plenary Assembly-Malaga Torremolinos, 8-19 October 1984; Geneva 1985; pp. 125-131

-Terminal Equipment 1 (TE1)- this includes all equipment that meets the CCITT defined ISDN interfaces to include data terminal equipment and digital telephones.

-Terminal Equipment 2 (TE2)- this includes all other equipment that do not conform to the CCITT defined ISDN interfaces. The prime contractor will provide the necessary interfaces to connect this equipment to the system.

-Network Termination 2 (NT2)- this includes key systems, PBXs, Local Area Networks (LAN), or switching cluster controllers.

System parameters for ISDN fall into two rate offerings, a basic rate and a primary rate. Both rates apply for circuit and packet modes of transmission. The basic rate provides each user with two 64 Kbps channels and a third 16 Kbps channel for signaling (2B+D). This rate would be delivered to TE1 and NT2 users at the CCITT defined T reference point while the TE2 user would interface at the R reference point. Conversely, the primary rate would provide the user with 1.544 Mbps divided into 23 channels of 64 Kbps (provided transparently) and one signaling channel (23B+D) or 24 channels with 64 Kbps (24B) controlled by associated signaling channel.

T-1 carrier interfaces consist of two types. Type 1 would employ standard pulse code modulation (PCM) schemes, following AT&T publications 62411 and 43801. This would include D3, D4 and Extended Superframe formats using channelization, framing format, signaling specifications and transmission performance of DS-1 signal. Type 2 would employ a low bit rate PCM providing 44 to 48 switched voice or data channels. This is especially designed for analog voice and slow speed data (4.8 Kbps) traffic. Any user equipment used in any of the specified services can interface the T-1 carrier either through the trunk side of a PBX, CENTREX or Central Office arrangement, or directly through the appropriate SDP.

Packet Switching. Provides users with packet switching services in both analog and digital formats,

synchronous and asynchronous. Packet switching services will abide by CCITT standards such as X.25, X.3, X.28, X.29 and ISO's Open System Interconnect (seven layer model).

User equipment interfacing this service would include:

-Data circuit-terminating equipment

-Data terminal equipment

-PBXs

Access to the network can be achieved either through dial up or dedicated connections. Dial up connections offer the user asynchronous data rates of 300, 1200 and 2400 bps, and synchronous data rates of 4800 bps, all in analog format. This would be employed mostly by off-net users, going on-net from a remote location over the PSN. For users on the network, a dedicated connection to the network is established, either through a PBX or direct to the network. This connection offers packet services in both analog and digital formats. Data transmitted on voice grade analog lines would get synchronous data rates up to 4.8 Kbps and 9.6 Kbps. Digital format lines would offer synchronous data services of 9.6 Kbps and 56/64 Kbps (when clear channel is available).

The packet switching service will offer electronic mail, a system to electronically store and forward text message traffic. This system will be compatible with telex systems and will have the capability for hard copy delivery.

Key parameters for the packet switching service include:

-24 hours/7 days a week service

-virtual and switched virtual circuits

-The option for contractor supplied packet assembler and disassembler at user's SDP

Video/Imaging Services. Provides the user with scheduled video and imaging services for conferencing in analog and digital formats. These services will be offered by utilizing both compressed and wideband techniques. With compressed video techniques, the signal is compressed/decompressed through video codec devises provided by the contractor. These codecs will be able to operate at 1.544 Mbps and 384 Kbps (eventually, 64 Kbps operation is desired). Furthermore, the codecs will be compatible with external encryption equipment supplied by the government to provide the user with the necessary transmission security. Compressed video transmissions will carry video, graphic, audio, and data information to meet the following requirements:

-one way point-to-point with audio return

-multi-point broadcast with audio return

-two-way point-to-point full-duplex interactive video.

Wideband video transmissions provide the same services as compressed video but on a much wider bandwidth, operating with a baseband of 6 MHz. In both compressed and wideband video services, the contractor will be in charge of scheduling system usage.

Dedicated Transmission Service. Provides user with dedicated transmission lines for voice, data and video in analog or digital formats, point to point or private line services. These

dedicated lines will connect to the FTS2000 network and access telecommunications service offerings directly.

Network Management Services

Network management services are provided by the prime contractor. Government oversight is handled through the Service Operation Center (SOC). The network management responsibilities are broken out as follows:[9]

Prime Contractor Responsibilities. The prime contractor is responsible for the operation and management of the network. The system user interfaces with the prime contractor through a Customer Service Office which will provide the necessary support to the system user. For system operation and oversight, the prime contractor will work with the government through the Service Operation Center (SOC). Among the management services provided by the prime contractor are:

-Customer Service and Administration and Support to interface with the user agencies for service orders, trouble reporting and complaints, training and documentation, technical support and user assistance.

-Billing functions through an automatic billing system for collecting, recording, formatting and distributing billing data by agency usage and location.

-Network Management and Control to include emergency service continuity and contingency planning.

-Technical Support. The contractor will establish a technical advisory center to resolve technical difficulties arising between the government, other systems interfacing the FTS2000, and the contractor.

Service Operation Center (SOC). This is the government control center within the network, protecting the governments interests in the system. The SOC interfaces with the contractor on operational and administrative matters. Its operational taskings include:

-Ensure contract compliance. The SOC is GSA's agent monitoring the system provider's compliance with the contract on a day-by-day basis. All prime contractor plans must come to the SOC for approval.

-Provide status of network performance. All network performance data is stored and managed by the SOC.

-Provide guidance for emergency situations. The SOC serves as the government's contingency center within the FTS2000. It is tasked with monitoring the contractor's emergency response plans. Additionally, it ensures the network staisfies national security and emergency preparedness requirements.

-Provide resolution of agency/prime service contractor problems not resolved through normal channels.

-Provide transition and implementation guidance. The SOC will monitor the transition process from the FTS to the FTS2000. All matters involving transition must come through the SOC for coordination and approval.

-Manage downsizing of FTS

The SOC's administrative functions include:

-Release payments to the prime service contractor

-Ensure network cost-effectiveness and usefulness. The SOC would handle this tasking by comparing vendors performance with other commercial service providers. Furthermore, the SOC will review network design and operation in an effort to identify shortcomings. Finally, it will promote new service requirements with the prime contractor.

-Monitor administrative contract compliance

National Security and Emergency Preparedness

National security and emergency preparedness (NSEP) outlines the federal government's response to national emergencies. These may include natural disasters, civil unrest, sabotage or terrorism, to direct attack against the US, affecting part of or the entire nation. The National Communications System (NCS) was established to meet the telecommunications needs of NSEP. The NCS specifies government telecommunications system must meet the following criteria to effectively function during emergency conditions:[10]

1. Responsive to national security needs of the President and federal Departments, agencies and other, including telecommunications in support of national security leadership and continuity of government.

2. Satisfy priority telecommunications requirements under all circumstances through use of commercial, government and private owned telecommunications resources.

3. Incorporate necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to ensure the survivability of the national security and emergency preparedness telecommunications in all circumstances including conditions of crisis or emergency

4. Is consistent, to maximum extent practical, with other national telecommunications policies

As an integrator of federal agencies, the FTS2000 forms a major part of the NCS network and must comply with these provisions. The following summarizes NSEP services provided by the FTS2000.[11]

Communications Security

The FTS2000 is not intended to be a secure network. It incorporates transmission protection for sensitive but unclassified message traffic. To provide this level of protection, GSA has specified that all transmission by terrestrial radio or satellite systems transiting, terminating or originating within the geographical areas of Washington DC, San Francisco and New York will be encrypted using NSA approved devices. If agencies require further protection, they must provide their own end-to-end coding devices. To facilitate this, the network is designed to be transparent to encrypted transmissions from user devices such as the Secure Telephone Unit III (STU III).

Data Base Security

The contractor must provide protection for data bases and information-processing systems critical to the operations of the FTS2000 network from unauthorized access by external means. Specific examples of sensitive areas include billing systems, critical user identification, authorization codes and classified locations. The contractor must provide protective measures up to security level Class (C2) as specified in NSA's "Orange Book" (Trusted Computer System Evaluation Criteria, DoD 5200.28-STD). Furthermore, the prime contractor must provide a liaison officer to coordinate with the SOC all matters relating to classified data and message handling. This liaison officer will be cleared at the Top Secret level.

Surge Capabilities

In an effort to operate in a shared network environment under emergency conditions, the FTS2000 system requires the following capabilities of its switched voice service:

1. System is required to carry 85% of the normal average business day load when:

-Locally focused offered load on the PSN is eight times the engineered normal load

-General FTS2000 offered load is 30% over normal

-National offered PSN load is twice engineered normal load

2. Loss of a single network switch will not disrupt more than 15% of the network traffic (except for switches serving Washington DC).

3. Protection of FTS2000 switching nodes from common control delays caused by PSN traffic using the same switches.

4. Ensure dial tone service from the local telephone company for FTS2000 users served by their Class 5 offices through either feature group D on-net access, public telephone off-to-on net access or other Class 5 services.

Circuit Restoral Priority

The FTS2000 will ascribe to circuit restoration priorities as prescribed in applicable government regulations with the eventual implementation of the Telecommunications Service Priority system.[12]

Network Survivability

The FTS2000 relies on the redundancy and robustness of the PSN to provide most of the network survivability. A key weakness with the PSN, though, is the vulnerability of its common channel signaling equipment trunks. These trunks combine all the necessary signaling features of the network in separate trunks to improve network efficiency and prevent unauthorized tampering through dial up circuits. However, should the network lose these trunks and their signaling information, the PSN could no longer operate. Currently, 90% of all signaling in the PSN is common channel and this number is rising.[13] To protect against this, the FTS2000 specifies that common channel signaling system paths will be protected through encryption (NSA approved) and redundancy. The same protection will be afforded to satellite

systems to protect their command and control links. These links control the satellite functions. Consequently, all satellite systems serving the FTS2000 launched after June 17, 1990 will have the capability of encrypting their command and control link to prevent system takeover by unauthorized agents.

Network Contingency Planning

The operation of the network rests with the contractor. To meet emergencies, the contractor will have a comprehensive plan on how to respond to surge conditions or system outages. Furthermore, the SOC will coordinate and approve this plan, serving as the government's network contingency center during crisis. Finally, procedures will be established to expedite network response to for rapid expansion during an emergency situation.

Critical User Options

The FTS2000 has two NSEP options to meet specific needs of critical users. The first, assured switched voice service, will guarantee system capacity during severe overloads to 1,000 critical users initially and eventually 10,000. These users will be assured 5% blocking or less during severe PSN and FTS2000 overloads as described in the surge capacity paragraph. The second option guarantees critical users specific routing of their access channels within the network. Called critical user access, this allows special users to identify the physical routes, direct connections to specific FTS2000 switches, and/or selection of particular types of channel facilities they require. This allows

critical users the ability to tailor their system transmission paths according to their unique requirements (survivability, security, etc.). Both option would be limited to only a select group of system users and controlled by GSA.

Service Pricing Schemes

The FTS2000 offers the government services priced on usage.[14] Pricing is divided by basic services and enhanced service offerings. Basic features include the six service offerings identified in the system description as well as NSEP requirements. These services are fixed by the contractor at levels not to exceed the lowest commercial rates available in a specific area. Enhance services include the special features and all other services beyond the basic offerings. This way, the FTS2000 user can plan for basic service costs at preestabished rates without worrying about sudden fluctuations in price. Then, the agency can shop among the numerous enhanced features to tailor their network to meet their needs and budget. The pricing scheme used for the FTS2000 is similar to the ones used on commercial networks.

Four basic factors affect the price charged for basic services: geographical location, traffic volume, time of day, and on-net versus off-net access. The first, geographical location, is based on the access area a call originates or terminates in. These access areas are fixed geographic locations established by the contractor (can be based on similar NPA-NXX numbering plan used by the PSN). Crossing these regions incurs access charges both at the

originating and the terminating ends which are included in the cost of service. The second factor, traffic volume, is based on the service used (data, voice, integrated, etc.) and the amount of capacity used. Time of day of usage also impacts price. GSA divides system usage into normal business day (Monday through Friday, 8 a.m. to 5 p.m.) and all other times (weekdays, 5 p.m. to 8 a.m., weekends and federal holidays). Finally, cost will depend on if the network is accessed from an off-net location or vice versus. Each of these factors will influence the price of basic services.

The enhanced service offerings include features and value added services available to the user on request. The price of these services is based on the feature itself and is independent to SDP costs, access area or network traffic volume charges. An example of this is the electronic mail system used in packet switching. The user pays a set fee for use of this feature. This fee is based on the feature itself and is not dependent on how often or how long it is used.

Typical charge for voice traffic would have a charge for the basic service and a fee for enhanced features such as attendant services and call screening. The basic charge would include:

-charges for transport across the access areas the call originated in and terminated in

-charge for transport across access areas

-charge for length of transmission

-charge for time of day the call is made

-charge for off-net connection or on-net connection (for example use of a dial-up modem for slow speed data from a PSN station accessing an FTS2000 station)

Fees for enhanced features would be added in to the overall system cost as an independent charge.

System costs include SOC, NSEP and network management functions. These costs are included as overhead in the user charges. Optional NSEP features, such as Critical User Access, are considered as enhanced services and charged directly to the using agency.

NOTES-CHAPTER IV

1. General Services Administration, Office of Information Resources Management; FTS2000 Services, A Request for Proposals to Replace the Federal Telecommunications System; Amendment 1; March 1987 (FTS2000 RFP)

2. Interview with Mr. Walter Irving, Information Resources Management Services, General Services Administration

3. FTS2000 RFP; section C.1

4. Ibid.; section B.1

5. US General Services Administration; Changes to Federal Telecommunications System (FTS) Intercity Services-Advanced Notification and Request for Comments; Federal Information Resources Management Regulation (FIRMR) Bulletin 29; 15 October 1985

6. FTS2000 RFP; section C.2.1.12

7. FTS2000 RFP; section C.2.1.7

8. FTS2000 RFP; section C.2

9. FTS2000 RFP; section C.3

10. Executive Order 12472; Assignment of National Security and Emergency Preparedness Functions; April 3, 1984

11. FTS2000 RFP; section C.6

12. Currently, circuit restoration priorities are specified in CFR 47, Part 213, calling for the restoration of common carrier channels before dedicated private line channels.. The Telecommunications Service Priority (TSP) is scheduled to replace this with a priority listing for restoring circuit outages.

13. Board on Telecommunications-Computer Applications, National Research Council; Nationwide Emergency Telecommunications Service for National Security

Telecommunications-Interim Report to the National Communications System; Washington DC; August 1987; pp. 19-20, 25

14. FTS2000 RFP; section B

CHAPTER V

PROBLEM AREAS

The FTS2000 has run into a series of problems that have delayed due dates for proposals three times and have now put the entire program on hold indefinitely. The issues surrounding the delays revolve around the criteria used by GSA in selecting the FTS2000.[1] The House Government Operations Committee and recently the Senate Government Affairs Committee have challenged GSA on their management of the program and their selection criteria in choosing a single service provider for such a large contract. First, Congress is concerned the government should be buying something for their money. Next, they feel giving the contract to a single vendor defeats the purpose of competition, putting government in a precarious negotiating position. Furthermore, Congress is concerned that a winning contractor would have control of a nationwide end-to-end network, defeating the basic intent of telecommunications deregulation. Congress bases many of these concerns on recent studies by the General Accounting Office (GAO) that have raised serious doubts about the leadership of the Office of Management and Budget and GSA in managing the federal government's telecommunications needs.[2]

This chapter summarizes the key issues delaying the implementation of the FTS2000 and proposes possible solutions. Both sides feel justified for their stance on the issues and time will tell which will win out.

Need for a Dedicated System?

Does the government need a dedicated telecommunications network in a highly competitive marketplace so rich in service offerings, and facing numerous regulatory changes equalizing the benefits of private and public networks? This is one of the questions being hotly debated in Washington at the writing of this thesis. Moreover, the results of this debate will have a great impact on future telecommunications acquisition policy within the government.

Purchasing or leasing a private system prior to the divestiture of the Bell Telephone Company offered the government many benefits. First, it was an effective way of getting needed enhancements and tailored services from a limited telecommunications marketplace. Bell Telephone Company, the regulated monopoly, was the only game in town. They set the price, quality and type of services available to the user. If an agency desired additional features, they had the option of purchasing a dedicated system such as a PBX to meet their specific needs. Furthermore, the government had full control over the equipment they purchased and over the cost of services they could then offer to the system user.

Another key advantage to owning a private network in the regulated environment of the 1960 and 1970's was an economic one. Before 1982, the Bell Telephone company controlled most long distance and and all local telephone services. For the general public to access long distance services, the Bell Telephone Co. imposed an "access charge" to recover the cost of utilizing the local exchanges to complete the long distance call. However, these charges did not apply to private networks. Furthermore, usage costs were not traffic sensitive. Therefore, a single line user was charged the same cost as a multiuser trunk accessing the switch. Both these advantages gave a high volume, private networks like the FTS a substantial cost advantage.[3]

With the changes in technology, and reassessment of access charges, dedicated networks have lost much of their appeal. First, technology has now made it possible to offer most of the enhanced services of the private network to the general public. Through software controlled switches, such as the #1ESS, #5ESS and Northern Telcom DMS-100, the public exchange carriers can now offer a diversity of services at reasonable costs. Moreover, with software control, the central office switch can tailor these services to fit the users needs. The common carriers can thus offer the benefits of a private network without the large capital investment to own and operate one. CENTREX is an example of such a service offering provided by most Bell Operating Companies (BOC).[4] Using a public or large telecommunications network for private network needs also removes much of the technological risks for users. With technology changing as fast as

it is now, a PBX or computer system can become obsolete before it is installed. As result, many firms are investing in services offered by the major telecommunications providers, such as the BOCs, instead of buying facilities and equipment.

A second challenge to private networks has resulted from changes in who pays the access charges for long distance services and traffic sensitive costs. Under the terms of divestiture and Modified Final Judgement, the non traffic sensitive customer costs were broken into two charges. The first, End User Common Line Charge (EUCLC), is a fixed monthly charge imposed on the user to recover local line costs. The second, Carrier Common Line Charge (CCLC), is a per-minute-of-use cost to reimburse the long distance carriers for their service. Presently, the Federal Communications Commission (FCC) is leaning toward imposing an access charge to private lines at both the originating and terminating ends of the long distance call. The FCC is also considering traffic sensitive billing schemes. These changes in tariff structure eliminate the large cost advantage once used to justify private networks.[5]

Private networks do serve important purposes essential to the government. First, economies of scale attained by combining agencies into one user group gives the government leverage in contract negotiations. The Kalba Bowen report showed the significant cost advantage a unified approach would have over a decentralized one.[6] Additionally, by bringing users under one system, each agency, no matter its size, can enjoy a wider variety of services than they could afford on their own (economies of scope). Thirdly, by concentrating management and control of the

network under one system, all agencies could reduce the size of their technical resources, saving time and money. Since the government is already short in these resources and now facing a dynamic marketplace, the option of a large private system is appealing.

Another key advantage to private networks is the unique interoperability and integration of services required by the government. Under NSEP, the federal government must count with a telecommunications network interconnecting its agencies across the nation. This could be achieved through decentralized acquisition of commercial services, but maintaining interoperability between agencies would be extremely difficult. GSA would have to exert massive and ongoing coordination efforts to ensure some semblance of connectivity is maintained. Furthermore, with the move of technology toward digital and ISDN, the government could face the risk of diverging systems. Unlike analog voice networks where most standards have been completed and implemented, digital technologies are still evolving. Discussions on standards used to integrate networks have not been resolved yet. However, industry is racing ahead with their versions of the standards in an effort to be part of this growing market. The resulting deviations in equipment and interface specifications could become a major obstacle to establishing a nationwide network managed by multiple vendors.[7]

The FTS2000 combines the advantages of a private network with the benefits of seeking industry provided services. Combining all government agencies under one system has given

the government powerful leverage. Futhermore, by building a single network, interoperability and integration of services can be realized without the coordination challenges of decentralized systems. Yet, by requesting state-of-the-art services, not hardware or facilities, GSA has passed the risks of changing technology onto the contractor. This ensures the government gets the latest enhanced features without having to purchase equipment or software. Since the FTS2000 shares the PSN with commercial users, the cost of these enhancements are shared across the network, making these services available to both the government and public user at competitive prices.

Single Versus Multivendor Provider

The biggest debate between GSA and Congress over this program deals with the importance of competition as selection criteria for the new system. Representative Brooks, chairman of the House Government Operations Committee, argues that the demise of the FTS was due to one contractor, AT&T, controlling a majority of the system.[8] He points out that the government is now hostage to AT&T's whims, driving up costs without the equivalent increase in service. Using the findings of the Kalba Bowen report and past experience, he feels the FTS2000 is too big a contract to offer to one vendor. Therefore, he insists the network should be split among multiple vendors to achieve true competition.[9]

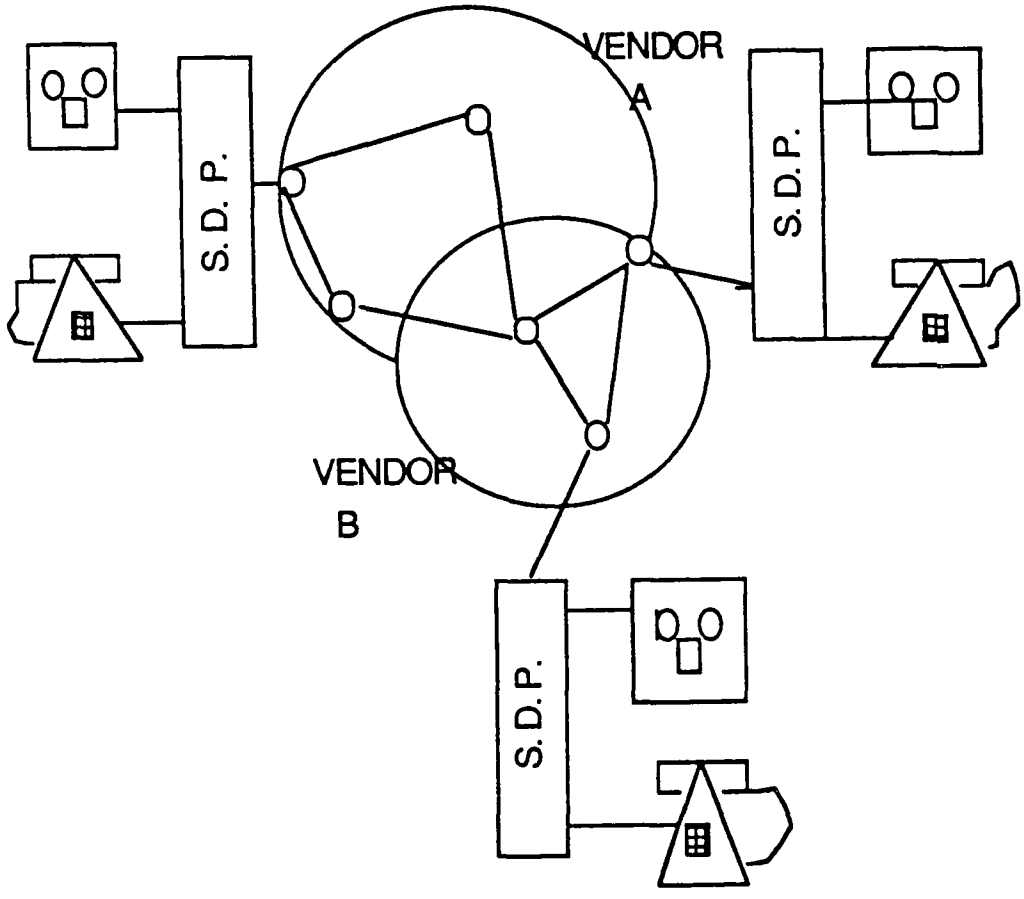
GSA, on the other hand, feels the contract contains all necessary terms to ensure the winning bidder is faced with incentives to offer competitive services.[10] Key to these terms is the voluntary role of the user and the four, seven and ten year intervals open for contract renegotiation. Under voluntary participation, any agency that finds similar services at lower costs is free to drop out of the network. GSA feels this would pressure the FTS2000 provider into reacting to the lower prices by dropping theirs. If not, GSA has the options to terminate the contract at three key timeframes, owing the contractor only 450 million dollars of switched voice service. This would prove painful to the contractor who has already made the investments to provide the other services and who would lose out on earning between 4 to 25 billion dollars of the government's telecommunications business over ten years. GSA feels this is sufficient leverage to keep the vendor competitive.

GSA's major concern is to maintain network integrity, favoring the one system provider over the multivendor approach. A single vendor would oversee the entire network, providing the necessary standardization and specifications to ensure interoperability. GSA would have one point of contact for any network change or update. Through the multivendor approach, though, GSA would have to monitor the contracts and operations of different system providers, a heavy burden they are trying to get away from. Secondly, interoperability and the move toward integration of services across the network would prove a greater challenge since GSA would need to actively coordinate every step

between contractors. Finally, with the move towards integration of services, GSA foresees difficult times in standardizing networks. Consequently, GSA feels the advantages of a single system integrator outweigh the unquantified benefits of a multivendor approach.[11]

If a multivendor approach is best, how should the network be split with minimum impact on system integrity yet provide the most competitive alternative? Congress has proposed either a geographical and an functional split (see Figure 5-1).[12] The geographical split would divide the network into two separate regions, one containing 70% of the network and the other containing the remaining 30%. As new services are required, GSA would award them to the vendor with the best service and price history. The problem with this approach is how do you physically split a software defined network the size of the FTS2000 and maintain overall system integrity? As each vendor wins and loses new business, their would no longer be clearly defined areas of responsibility, complicating network management for the contractors and the government.

The second approach calls for splitting the network 70%/30% along functional/agency lines. Each segment would have a different vendor. Vendor performance would be measured by comparing each against the other. This "yardstick competition" would then promote the desired competition. Again, GSA questions this approach on the grounds of interoperabity between agencies. They point out this approach would weaken the government's advantages in economies of scale and scope.



GEOGRAPHICAL/FUNCTIONAL SPLIT OF THE FTS2000 NETWORK

Figure 5-1

Furthermore, GSA would have to maintain a more active role in oversight and coordination between the different vendors to ensure the smooth operations of the network. The debate continues as both sides stand by their decision.

Impact on Deregulation

A third concern with the FTS2000 is how will it impact the spirit of deregulation? 1982 signaled a major step in the government's steady move to deregulate the telecommunications industry. As result of the Modified Final Judgement with the Department of Justice (DoJ), the Bell Telephone Company was split up into local loop providers (RBOCs) and long distance provider (AT&T).[14] The purpose of this move was to break up the Bell Telephone Co. monopoly, therefore promoting competition in the long distance market while maintaining the basic regulated services of the local loop. By doing this, the government eliminated the last major obstacle to a deregulated marketplace. With no one entity controlling a nationwide, end-to-end network, coupled with the evolving technology, the government hoped to finally ensure competition in the telecommunications industry. The results so far have been positive with an explosion in telecommunications offerings and vendors. How would a major network the size of the FTS2000 impact this growing marketplace? Under this program, the winning bidder would earn the right to build an end-to-end telecommunications system which it would then be free to offer to commercial customers as

well as to the government. Many feel this would give the winner the monopolistic advantage the Bell Telepone Company enjoyed prior to divestiture. How true are these fears cannot be quantified at this time but must be considered in the decision process.

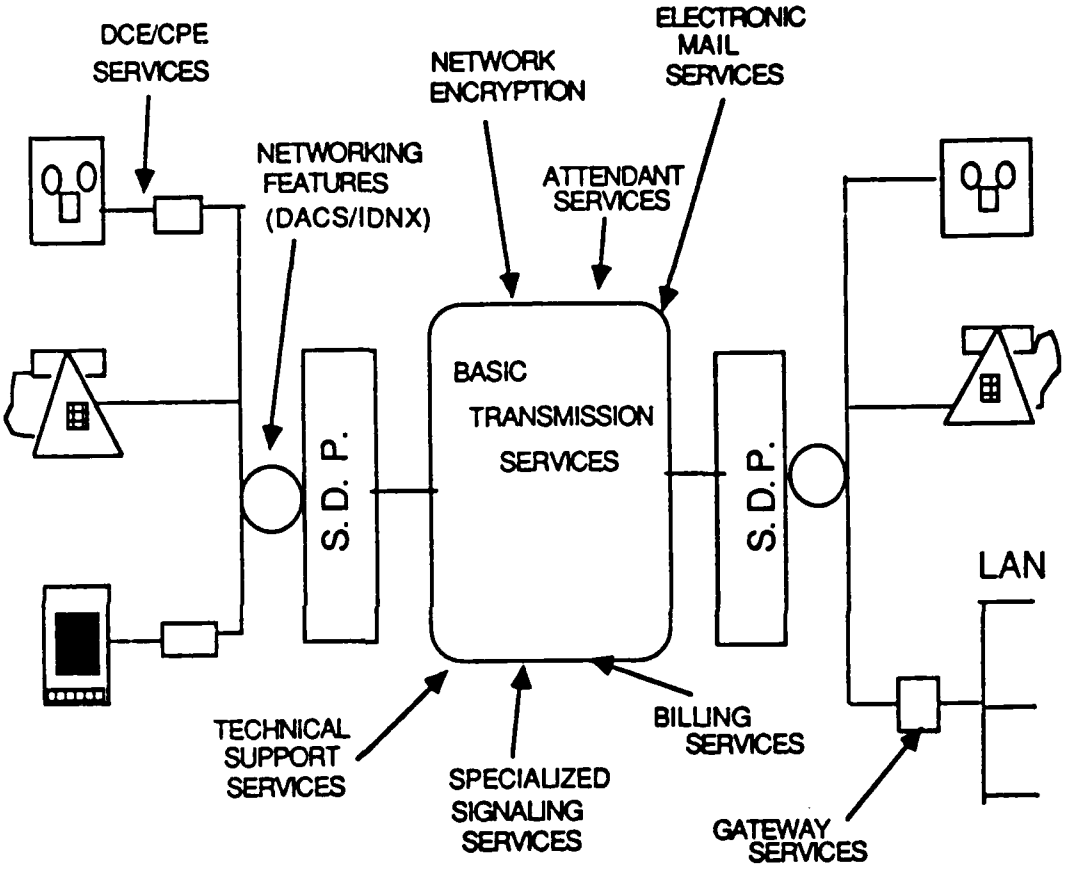
Another problem arising with the FTS2000 is the role of the Regional Bell Operating Companies (RBOC) in intercity, value added networks. In Computer Inquiry II, FCC defined network services as basic and enhanced.[15] Basic services were those required to transmit the information without modifying the message itself. Enhanced services were those that modified the message during transmission. Examples of basic services would are the transmission circuit paths on which traffic is routed while enhanced services include the specialized features that manipulate these transmission such as call queuing, attendant services or electronic mail. FCC specified that the local loop carriers could only offer basic services, thus providing a transmission "pipeline" on which other service providers could apply enhanced services. The DoJ upheld this decision in the divestiture proceedings and continues to monitor the RBOCs for compliance. AT&T is now using this decision against the other bidders, stating that by involving the RBOCs in their groups, they are letting them participate in enhanced service offerings, thus violating the intent of the divestiture rulings.[16]

A possible solution to the issue on how to best split the network to foster competition could lie in using the deregulation process coupled with the multivendor approach advocated by

Congress. This solution may lie in maintaining a single vendor providing a network of basic transmission services while competing all the other services (see Figure 5-2). The basic system vendor would provide a nationwide network of transparent transmission "pipes" on which any service or information could travel. This is a major undertaking for all but a few entities such as AT&T or Martin Marietta, limiting competition. However, enhanced services vary in size and complexity, and would offer companies large and small an opportunity to compete. This approach would thus maintain system interoperability while providing greater opportunities for competition in an area rich in vendors and service offerings. GSA could accomplish this by specifying that the winning bidder must subcontract all services except the basic ones or by making separate contracts for different services. By doing this, GSA would still maintain centralized control over the network, ensuring its transparency to enhanced services, while fostering greater competition.

Apparent Lack of Leadership in Integrating the Federal Government's Telecommunications

GAO published a series of reports questioning GSA and OMB's leadership in meeting the governments telecommunications needs.[17] Their findings pointed out a lack of long term planning or direction for telecommunications, lack of adequate criteria



SYSTEM SPLIT OF THE FTS2000 NETWORK

Figure 5-2

(standards and evaluation tools) for individual agencies to use in pursuing telecommunications systems, and lack of action to ensure existing policies were followed. GAO concluded that since neither agency had met their commitments, all telecommunications procurement actions were questionable and should be halted until they could be carefully analyzed. The FTS2000 was one of these actions. Again, GAO pointed out that a multivendor approach would prove more beneficial to the government by fostering competition not possible in the single vendor approach.[18] In a later report, GAO changed its position slightly, stating that the FTS2000 would be adequate in the short term (4 years), but that a long term solution would still be necessary.[19] Representative Brooks stands by the original report and has used it as ammunition in his battle with GSA.[20]

I believe GAO studies failed to take into account all major government telecommunications providers in their study. Key among the missing organizations were the military and NCS. Currently, GSA and the military operate major telecommunications networks as well as a myriad of smaller ones in the US. Unfortunately, few of them can interoperate with the others except through specialized gateways or an attendant console. This considerably limits the connectivity of the government in times of crisis such as those foreseen by the NSEP. Moreover, even though this arrangement is workable with analog voice systems, it poses serious techinical problems for digital technologies. It eliminates most of the advantages of speed, integration, and economies achieved through use of digital over analog techniques.

most of the advantages of speed, integration, and economies achieved through use of digital over analog techniques.

The NCS is tasked with ensuring government networks are interoperable and standardized.[21] Yet, separate networks continue to proliferate without a centralized effort to integrate them. The NCS, along with OMB, GSA and the military should look into this larger problem to find ways to improve cooperation and standardization between agencies and move toward integrating networks. Only through this effort can a truely integrative program for federal telcommunications, as proposed by GAO, be attained.

NOTES-CHAPTER V

1. Conversations Mr. Walter Irving, Information Resources Management Services, General Services Administration and Mr. Charles Wheeler, House Government Operations Committee

2. US General Accounting Office, Information Management and Technology Division, ; Information Management, Leadership Needed in Managing Federal Telecommunications; IMTEC-87-9; May 6, 1987

3. Kalba Bowen Associates, Inc and Economics & Technology, Inc.; Cost/Benefit Analysis of Aternatives for the Replacement of the Federal Telecommunications System Intercity Network; Volumes I, II and III; May 30, 1986

4. AT&T Bell Laboratories; Engineering and Operations in the Bell System; Second Edition; 1983; pp. 67-70

5. Kalba Bowen Associates Inc.; Volume II-"Criterias, Alternatives, Evaluation"; *Appendix II*

6. Ibid.; Volume I-"Executive Summary"; pp. 7-8, 18-20

7. The implementation of ISDN is an example of this problem. The standardization process is voluntary and many times is a compromise position. ISDN is an example of this problem. Even though there are standards for ISDN implementation, such as X.25, there are many alternate means of applying the standard. A system can meet all requirements within the X.25 standard yet not be compatible with another X.25 standardized system. For more information on this subject, see Edwin E. Meir; "Compatibility Becomes a Growing Concern for ISDN's Future"; Data Communications; November 1985; pp. 64-74

8. Since his intervention, the Senate Government Affairs Committee has also taken an interest in this matter, backing Rep Brooks on selection of the multivendor vrs. single vendor approach.

9. From conversation with Mr. Charles Wheeler, House Government Operations Committee

10. From conversations with Mr. Walter Irving, GSA

11. Ibid.

12. From conversations with Mr. Charles Wheeler, House Government Operations Committee and Mr. Walter Irving, GSA

13. Since finishing this thesis, the House Government Operations and the Senate Government Affairs Committees have made GSA reconsider its decision in favor of a multivendor approach. As of October 22, 1987, GSA is still trying to figure out how best to split the network in order to provide the needed competition without loss of system integrity. Roy D. Rosner in "Network Managers Play Humpty Dumpty"; Government Computer News; October 23, 1987; pp.52, 77-78; sees agencies breaking away as FTS2000 if delayed further.

14. US vrs. American Telephone and Telegraph Co., 552 F. Supp 131 (D.D.C. 1982) aff'd sub nom. Maryland vrs. US, 460 U.S. 1001 (1983)

15. Second Computer Inquiry, Final Decision, 77 FCC 2d at 420, para 93 (Basic services) and 47 C.F.R. Sec, 64.702(a) (Enhanced services)

16. Bonafield, Christine; "AT&T Protest Raises FTS2000 Issue"; Communication Week; June 22, 1987; No. 59; p. 8

17. The primary document in which the findings are summarized is US General Accounting Office report IMTEC-87-9 titled Information Management, Leadership Needed in Managing Federal Telecommunications; May 6, 1987; pp. 48-51

18. Ibid.; pp. 19-20

19. Conclusions and recommendations from US General Accounting Office, Information Management and Technology Division report Information Management, Status of GSA's FTS2000 Procurement, IMTEC-87-42; August 1987; pp. 6-8

20. From conversations with Mr. Charles Wheeler, House Government Operations Committee and Mr. Walter Irving, GSA

21. Executive Order 12472; Assignment of National Security and Emergency Preparedness Functions; April 3, 1984

CHAPTER VI

FTS2000, A MILITARY PERSPECTIVE

The FTS2000 remains a viable solution to the government's telecommunications needs. Furthermore, it is backed by over 95 federal agencies.[1] One large federal entity is absent in the user lineup: the military. The Office of Secretary of Defense and the Defense Communications Agency (DCA) have endorsed the program for their use, yet the military as a whole has remained uncommitted, pursuing instead its own network solutions.[2]

This chapter addresses the issue of why the military should reconsider its decision and remain involved in the FTS2000 program. By using the FTS2000, the military could achieve many benefits while working towards a more cohesive telecommunications sytem, a key goal of the federal government as a whole.

What Does The FTS2000 Offer the Military?

The military has relied on two major long haul telecommunications networks for the last 25 years, AUTOVON and AUTODIN. These networks have undergone numerous updates and are now being replaced by newer voice and data

systems. The Defense Commercial Telecommunications Network (DCTN), is one such interim network solution, offering voice, data and video services through a private system provider, AT&T. The Defense Communications Agency, the military long haul communications provider, is now developing the Defense Switched Network to replace AUTOVON and DCTN as well as serving as the transmission network for other defense telecommunications systems by the year 1995. Some of these other networks include the Defense Data Network (DDN), a leased packet switching service to meet the needs of the military's mini and microcomputer communities. A second is the Interservice Integrated Automatic Message Processing Equipment (IS/IAMPE) program which will replace AUTODIN as the military's message traffic carrier. Both DDN and IS/IAMPE are value added services and will utilize DSN as their transmission network. DSN parallels the FTS2000 in that the military is moving away from dedicated facilities in favor of leased services.[3] With an overall military telecommunications expenditures in the US valued at over 2 billions dollars a year, this move will prove an interesting opportunity for commercial service providers.[4]

What does the FTS2000 offer the military that it cannot already achieve through their existing networks? I believe the military and the federal government would realize the following benefits should they work together on the FTS2000 program:

Further the objectives of national security and emergency preparedness (NSEP).

NSEP requires a nationwide response to effectively respond to whatever crisis the US may face. This entails federal agencies working together at all levels of command. To effectively coordinate this effort, NSEP specifies the need for interoperable and redundant communications to effectively link nationwide agencies into a cohesive and survivable network.[5] One of the key purposes for the FTS2000 is to provide the federal government with such a network. It combines voice, data, video and packet switching resources into one network. Through its on-net and off-net capabilities, it gives crisis action teams telecommunications services anywhere they can interface the public switching network.

Presently, the military networks have limited connectivity to the rest of the federal government. Should an emergency arise, crisis managers have to interface with numerous networks simultaneously in an effort to coordinate any action. Unfortunately, most of this connectivity is only at the highest levels of authority. The actual action teams lack necessary telecommunications tools to integrate response efforts, complicating coordination and rapid resolution of even the smallest emergency.[6] Should the military become part of this network, NSEP authorities would have clear access to all federal agencies at all levels of response through a single system whenever they need it.

Integration of federal telecommunications resources.

The FTS2000 program incorporates all services offered by the diverse defense long-haul networks into one system. Its architecture, based on services through the public switching network, provides flexibility, growth and interoperability to its users. Furthermore, this network will be available by 1990 versus the 1995 target date for DSN. The military would therefore benefit from a network rich in services, interoperable with the federal government as a whole, and available within the next two years.

Ensure standardization of the federal governments telecommunications networks.

This standardization effort would encompass:

Technical standards: With the rapidly changing technology in the telecommunications marketplace, equipment standards offered by different vendors may vary. This is due to differing interpretations of standards. Consequently, separate networks boasting the same services could diverge as technologies varied, leading to eventual loss of connectivity.[7] By using the same network, the federal government would be assured connectivity with minimum coordination effort.

Standardized government numbering plans. A big problem to linking the different federal networks is the lack of a standard numbering plan. Standardized numbering plans have proven key in unifying the various segments of the PSN into one system.[8]

The government would gain much of the same benefits by giving each government user a specific station number.

Standardize network software. Network management is now software controlled. Variation in network software could result in certain incompatibility of networks. Again, with the military participating with the rest of the federal government on software compatible networks, true interoperability and connectivity can be achieved.

Standardize interfaces. A second major strength of the connectivity of the PSN is commonality of interfaces.[9] This would give vendors a common set of specifications for all government systems. The resulting commonality of hardware available to the government would drop overall production and installation costs. Furthermore, this would give system providers of specialized and foreign networks clear specifications to integrate their systems into the government one. The PSN, through standardized interfaces, has not only integrated the numerous service providers in the US into the network, but also linked to foreign and specialized systems, achieving true interoperability.

Coordinated migration of federal telecommunications towards integration of services

ISDN will offer telecommunications users large, high-speed and transparent information highways, linking the nation to the world. The key to successful implementation of ISDN, though, is for the large volume users to lead the way. ISDN has faced serious

delays in the US because the decentralized telecommunications industry is fighting over the interpretation of the standards.[10] A coordinated effort by the largest private network in the US, the federal government, could ensure ISDN finally gets a footing and grows to its full potential. Should this effort be split up among competing government agencies without a single system integrator, the resulting networks could end up with such diverging technologies they would be completely imcompatible, defeating any hopes for ISDN's success.[11]

Best utilization of federal telecommunications resources

As discussed in previous chapters, the fiscal realities facing the government are grim.[12] Shortages of qualified technicians, severe budget cutbacks and the move toward privatization of services are forcing the government to rethink how it does business. By combining federal telecommunications efforts into one cooperative venture, current redundancies and waste could be eliminated while saving costs, personnel and effort for all.

Move towards a truly integrated telecommunications policy for the federal government

GAO, in its report to the House Government Operations Committee on the management of federal telecommunications, indicated that OMB and GSA had fallen short in providing leadership for this critical area. GAO concluded that both agencies should take a more active role in planning and implementing an integrated approach to meet the government's

telecommunications needs, present and future.[13] With a telecommunications budget in the billions of dollars and similiar network requirements, the military forms a major part of the government telecommunications usage. Therefore, the military's participation in this process is essential to guarentee true integration is achieved.

In conclusion, the military's involvement in the FTS2000 program would bring benefits not only for itself and the system, but for the integration of government telecommunications as a whole.

Military Concerns with the FTS2000 Program

In his February 25, 1986 letter to GSA, Mr Donald Latham, Assistant Secretary for Defense, Command Control Communications and Intelligence ($ASDC^3I$), stated the military's position on the FTS and the FTS2000 program. Concerning FTS, he says:

> ....the Department of Defense (DoD) continues to consider alternative approaches to obtaining high quality telecommunication services at minimum cost. Consequently, use of their Federal Telecommunication System (FTS) by the DoD may not continue at the current level as we evaluate the quality and costs of alternative services. The DoD's primary telecommunications concern is reponsive communications in support of military operations, exercise of command and control, and national security....Flexibility, especially in today's rapidly changing telecommunication environment, will also be critical to obtaining economical service. For these reason the DoD cannot agree to enter into a three-year service agreement for FTS services.

Regarding the FTS2000 program, he then states:

> DoD will continue to consider alternative approaches to obtaining high quality telecommunication services at minimum cost....For these requirements, we will evaluate the FTS2000 services when it is under contract, and compete its service offering with those of other service probviders to satisfy our needs in the most economical way.

Therefore, the military is seeking other ways to meet its unique requirements but has not rejected th FTS2000 program altogether. The question is, what are these special requirements the military has that the FTS2000 cannot meet?

DoD, because its unique taskings and system threats, specifies its telecommunications networks must meet a series of specialized features known as military unique features (MUF).[14] These MUFs include increased security and precedence and surge response to enable it to operate in a hostile environment during threats to national security.

Added Precedence/Priority Requirements

The military specifies Multi Level Precedence and Priority (MLPP) is mandatory. This MUF requires an automatic system of priority call and restoration of essential trunks and/or lines taking precedence over all other trunks and/or lines of lower precedence transversing the system. The military also requires all connections to military installations and interswitch trunk groups have this capability. Functioning within the PSN, this would mean the military call of high enough precedence would preempt any call on the switch, private or dedicated, should all trunks be

occupied at the time in an effort to ensure its completion. Upon switch outage, these circuits would take priority over the common carrier or dedicated ones for restoral.

Presently, under Federal Communications Commission Orders 69-1113, restoration of PSN channels have higher priority than dedicated private circuits. This means MLPP is not possible under current FCC directives. Therefore, until the FCC reverses its decision, priority calling is achieved through precedence queuing in which circuit priorities within the dedicated network itself are established. During restoration, this listing is followed manually to achieve the required precedence. The FTS2000 Request for Proposal (RFP) specifies this restoration criteria will be in effect until the new Telecommunications Service Priority program is in place.[15]

A solution to the precedence problem can be achieved through software found in the newer digital signaling systems such as Common Channel Signaling System No. 7 (CCS#7). These software fixes are now under consideration and will form a major part of ISDN and the FTS2000 specifies CCS#7 as the network signaling system. As the network migrates toward ISDN, which utilizes CCS#7 as the heart of its network, advanced precedence features could be attained at a relatively low cost.

Additional Surge Capability

On the average, the MUFs call for the network to operate with a 50% increase in traffic load over peacetime loads in a crisis situation. However, key locations will require an increased surge

capability of up to 150% over peacetime capacity during special conditions and for short intervals. Additionally, the MUF requires sustained 75% to 100% focused overloads over extended periods of time. The FTS2000 RFP call for the network to handle an 85% load increase over normal peacetime load during crisis. Additional surge requirements are possible but costly.[16]

Added Security Measures

DoD is especially concerned with network security measures. The MUFs require the reduction of security risks during system development and the protection of sites and data bases once the system is operational. This would include security clearances and/or reliability checks on development personnel; security checks on software, system and configuration management during development; and site security involving encryption of vulnerable circuits, data bases and remote maintenance access. The level of security contermeasure capabilities desired is NSA class C-2 (Orange Book) in the near term with the eventual upgrade to class B.[17]

GSA's approach to security is to provide the user with a robust network, transparent to any government cryptographic equipment. The user then furnishs its own end-to-end security protection. GSA's philosophy on network encryption is that it would be highly expensive and technically complex to satisfy only a small part of the system's load.[18] Currently, the FTS2000 RFP calls for the equivalent of NSA C-2 protection of data bases only. It does specify the protection of critical circuits but only within

certain geographical areas and only to the level of SENSITIVE. GSA does not have a special plan to ensure security reduction measures are included during the network's development, implementation or eventual operation. However, it has specified the contractor will be responsible for material to the level of Top Secret and should have personnel and facilities cleared to handle classified material.[19]

Interoperability to Other Military Systems

The military has a worldwide mission, integrating the efforts of military units in the continental US and overseas with those of allied armed forces, such as NATO. To do this, the military must interface with numerous networks such as TRI-TAC (tactical command and control system), the international DSN networks (Europe, Pacific, Southern, etc), NETS and the Canadian military networks. Along with the interfaces comes the need for a standard worldwide numbering and overseas gateway operation.

Interoperability is a key concern of the FTS2000 program. The FTS2000 currently is configured to handle AUTOVON and DSN. Furthermore, with the move in DDN to make it compatible with X.25 networks, DDN would be able to interface with the FTS2000 network. DDN is a value added service and travels any network capable of handling its unique protocol arrangements. FTS2000 could provide this type of a network.[20] Additionally, FTS2000 specifies the need for interoperability with NETS once it becomes available and is made a required part of government networks. To date, the military has not specified to GSA the need for the

FTS2000 program to be interoperable with other military systems. However, GSA states these additional networks can be added to the program if necessary.[21]

FTS2000 specifies an universal numbering plan to accomplish the necessary interoperability. The military's participation in this effort is key to the successful connectivity of these diverse networks.

Added Survivability Measures

The military's key concern is for sabotage or terrorism attacks on its networks. To avoid system degradation due to these threats, the MUFs require all networks to be dual-homed services, contain survivable and encrypted signaling system, and provide increased protection of physical site and personnel security. The FTS2000 meets most of these features with the current contract. A major discrepancy exists with physical protective measures, though. GSA has specified that protective measures currently enforced throughout the PSN are sufficient and the true network survivability comes from its robustness.[22] DoD wants greater protection and hardening of key switching and transmission sites.

The NCS is addressing the issue of network survivability through their Network Emergency Telecommunications Service. NETS will provide 20,000 authorized federal government users with survivable switched voice and slow-speed data communications. NETS will operate in the pre-, trans-and post-attack enviornement to provide the US with the necessary communications after a large-scale nuclear attack. Taking

advantage of the PSN's ubiquity, geographic diversity and robustness, NETS will upgrade its survivability through hardware and software modifications. Using special routing devices installed at key nodes, authorized calls will be routed through all possible transmission paths until the call is completed. This will give the government the necessary connectivity to survive partial damage to the PSN during a national emergency or attack.[23] To date, this network is still in the experimental phase and is not a requirement for government networks. The DSN and FTS2000 RFP lists connectivity witn NETS as desirable in the future, leaving open the option to interconnect it into the network at a later date.

Other Concerns

Apart from the technical problems, DoD is concerned with the need for a multiple year commitment required by GSA for initial participation in the FTS2000 program.[24] Under current terms, participating agencies must commit to four years with the new system to assure the contractor a minimum usage rate. DoD does not want to be stuck with a multiyear commitment for a system that is still unproven. Furthermore, this would commit funds that could be used elsewhere.

Finally, the Department of Navy has voiced concern about the FTS2000 billing system.[25] The Navy wants the telecommunications billing data broken out by the lowest using organization instead of the FTS2000 method of billing by agency. This approach puts the burden of tracking costs on the Navy. GSA

argues that billing by agency is less costly and easier to implement since the current pricing schemes vary in complexity, depending on the service used.[26] Again, should the military form part of the FTS2000 program, its size as a user group would give it necessary leverage to pursue its demands.

The military and the government as a whole have much to gain by all agencies joining an FTS2000 program. These benefits include efficiency, interoperability standardization, cost savings and the move towards an integrated federal telecommunications policy. However, the military asserts the FTS2000 program does not meet all of its requirements. Are there alternatives and options both GSA and the military should examine to resolve these differences while achieving the benefits of a cooperative approach? The next chapter explores some of these alternatives and options.

NOTES-CHAPTER VI

1. Christine Bonafield; "GSA Proposes Oferring Agencies Another Chance to Join FTS2000"; Communication Week; April 13, 1987; No. 139; p. 85

2. Ibid.

3. Christine Bonafield; "Defense Plans Would Create Billion-Dollar Carrier Contracts"; Communication Week; April 13, 1987; No. 139; p. 1, 85

4. Ibid.

5. Executive Order 12472; Assignment of National Security and Emergency Preparedness Functions; April 3, 1984

6. See Chapter II, "AUTOVON"

7. Meir, Edwin E.; "Compatibility Becomes a Growing Concern for ISDN's Future"; Data Communications; Nov 1985; pp. 64-74

8. Board on Telecommunications-Computer Applications, National Research Council; Nationwide Emergency Telecommunications Service for National Security Telecommunications-Interim Report to the National Communications System; DC; August 1987; pp. 15-16

9. Ibid.; p. 16

10. Walt Sapronov; "Technical and Regulatory Issues Challenging ISDN's Progress"; Data Communications; November 1985; pp. 265-274

11. From conversations with Walter Irving, Information Resources Management Services, General Services Administration. GSA's greatest concern is network integration, without which an interoperable system could not be achieved.

12. With the passage of the new Gramm-Rudman-Hollings Balanced Budget Act as amended on September 29, 1987, the government is committed to balancing the federal budget by the

year 1993. Budget cuts for 1988 are estimated at 23 billion dollars. This means a 12.4 billion dollar cut in defense spending alone, dropping their budget up to 4 billion dollars below 1987's budget. This has made government planners rethink how theyspend their money. (see Elizabeth Wehr; "Democrats: Snared in a Gramm-Rudman Trap?"; Congressional Quareterly, Weekly Report; Vol 45, No 40; October 3, 1987; pp. 2394-2395

13. US General Accounting Office, Information Management and Technology Division, ; Information Management, Leadership Needed in Managing Federal Telecommunications; IMTEC-87-9; May 6, 1987

14. Defense Communications Agency; The Defense Switched Network Program Plan, FY 1989-1993 enumerates various requirements unique to military systems.

15. US General Services Administration, Office of Information Resources Management; FTS2000 Services, A Request for Proposals to Replace the Federal Telecommunications System; Amendment 1; March 1987; Section C.6.2.6

16. FTS2000 RFP, Section C.6.5. and from conversation with Mr. Walter Irving, GSA.

17. These parameters specify required countermeasure capabilities and procedures within a network to achieve protection against a specific level of enemy threats and are outlined in DoD 5200.28-STD, Trusted Computer System Evaluation Criteria.

18. Conversations with Mr. Walter Irving, GSA

19. FTS2000 RFP, Section C.6.5

20. The DDN is a value added service using TELNET to transmit its traffic load. DDN utilizes TCP/IP protocol but is migrating to the ISO OSI seven layer model which uses CCITT X.25 packet switching protocols. From conversations with Mr. Steve Wolf; Director, Networking, Communications, Research and Infrastructure Division; National Science Foundation; Internet, the scientific network using ARPANET, software modifications on the network layers (1 to 3) to fit X.25 protocol have been very

successful in making the transition and are presently in use. (for more information on DDN, see The DDN Course, by Network Strategies, Inc.; Contract DCA-100-83-C-0062; April 1986

21. From conversation with Mr. Walter Irving, GSA

22. Ibid.

23. Nationwide Emergency Telecommunications Service for National Security Telecommunications-Interim Report to the National Communications System; August 1987; pp. 6-14

24. Christine Bonafield; "GSA Proposes Oferring Agencies Another Chance to Join FTS2000"; Communication Week; April 13, 1987; No. 139; p. 85

25. From conversations with Irving, Walter, GSA. Robert L. Ellis in his article, "Will GSA Defend Its Honor or Arrive Empty-Handed?; Government Computer News; October 23, 1987; pp. 50, 65; outlines the complexity of the billing system.

26. Ibid.

CHAPTER VII

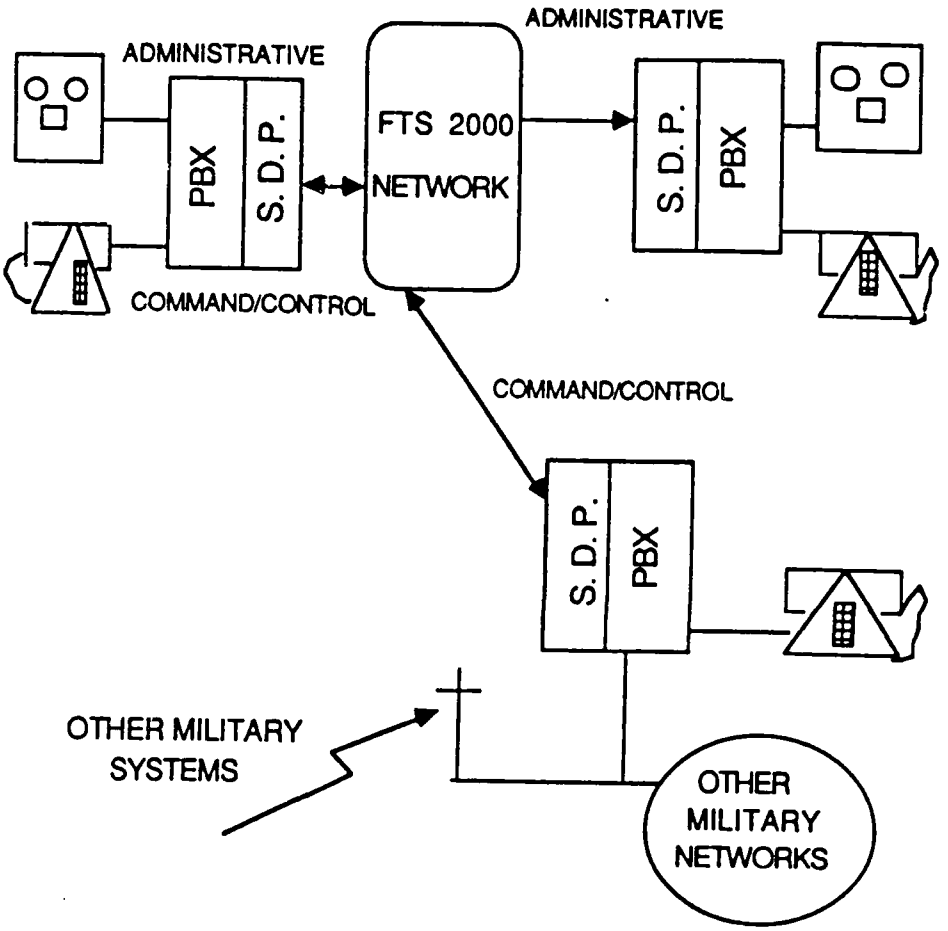
ALTERNATIVES AND OPTIONS

The FTS2000 offers the federal government through a system rich in connectivity and services. How can the military take advantage and become part of this effort? This chapter proposes a number of system alternatives as well as security and survivability options for the military to consider. Each is described in general detail and then analyzed from a military planners perspective. Though each alternative may have its drawbacks, one or a combination of alternatives could provide the government true connectivity at a reasonable price.

System Alternatives

Route all Military Traffic over the FTS2000 (Figure 7-1)

Under this alternative, the military would utilize the FTS2000 network to route all their administrative and command and control (C^2) traffic. The administrative traffic load would fit the network as it is now configured. The C^2 load, however, would require additional features to those now found in the FTS2000 program.



ROUTE ALL MILITARY TRAFFIC THROUGH THE FTS2000 NETWORK

Figure 7-1

Utilizing funding and resources now employed in developing separate, dedicated networks, military planners could achieve the added features required by the C^2 network users. Among these features are precedence and priority systems, better congestion control mechanisms, added security measures, and interoperability with other military systems. Higher precedences and priorities could be accommodated through NSEP optional features such as Assured Switched Voice Service for Critical Users and Critical User Access.[1] Furthermore, by subscribing to the NCS's National Emergency Telecommunications System (NETS),[2] both the military and the federal government would receive added connectivity across the PSN during times of national emergencies as well as for exercises. The FTS2000 network could achieve greater congestion control by incorporating additional mechanisms across the entire network or on specific segments, ensuring critical capacity to users when needed. Increased security measures on the network could be accomplished by implementing one of many security options discussed later in this chapter. Finally, the network could be interfaced with military unique systems using of gateways, selected entry points, or modifications to system protocols.[3] These points could be located within the network itself or at military switches interfacing the network. Utilizing a universal numbering plan and authorization codes, government users could access any system, military or non-military, from any point in the FTS2000 network.

By integrating its enormous traffic load into the FTS2000 program, the military would gain tremendous leverage over the

system. DCA Networks estimates the military's requirements would make it the largest FTS2000 user with approximately 50% of the system's traffic load.[4] Using this as leverage, the military could have greater influence on the operations of the network. Working closely with GSA, DCA would become an active partner on network decisions and a permanent member in the Systems Oversight Center (SOC).

The advantages of this alternative are:

-Interoperability among the entire federal government would provide true connectivity sought under the NSEP.

-Eliminate the investment and risk to the military of separate, dedicated networks

-Increased economy of scales for the FTS2000 program with military's participation. This would translate into greater bargaining leverage to lower costs while improving services.

-Share the advantages offered from the FTS2000 program such as connectivity, flexibility, and state-of-the-art services.

-Money saved from building separate military networks could be used to provide new services to the military on the FTS2000, procure needed military telecommunications project or for other military programs.

-Features added to the system for the military could potentially benefit other federal agencies as well.

-Progress towards integration would be easily implemented and would serve all federal agencies.

The disadvantages of this approach are:

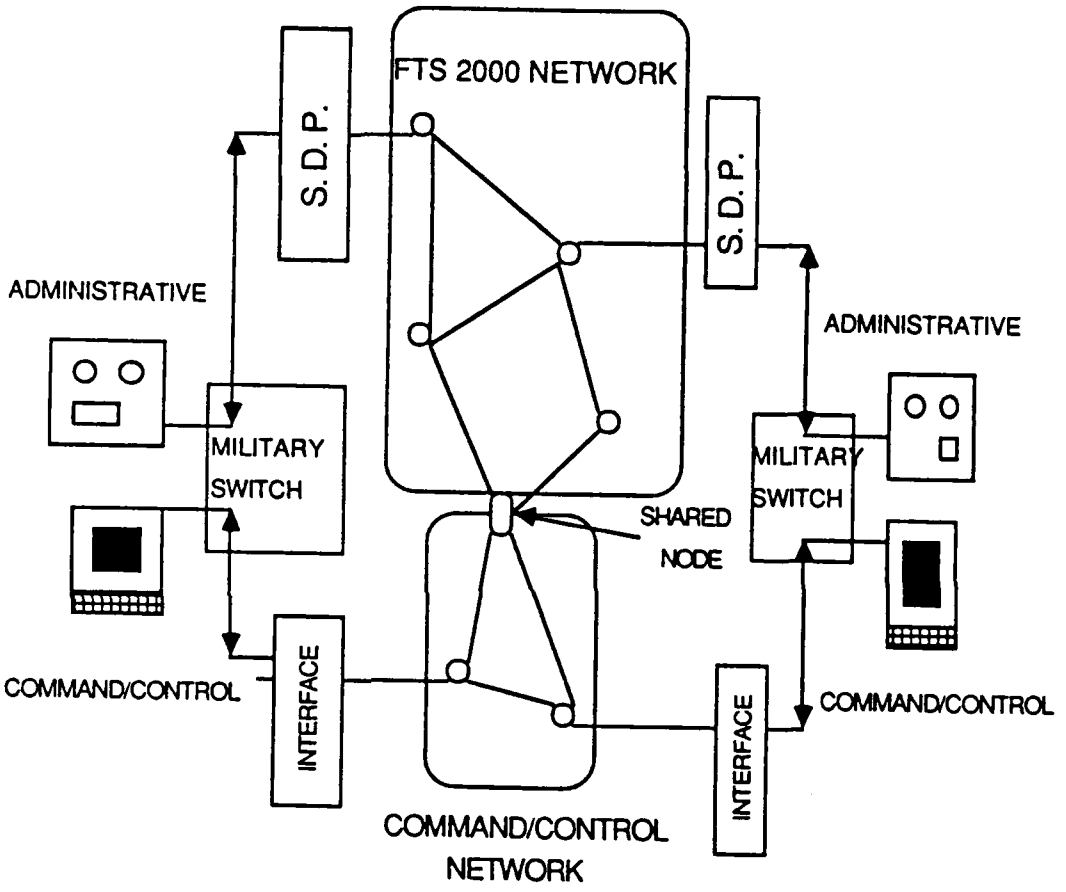
-By not owning the FTS2000, the military would have to bargain with other government agencies to attain necessary changes to the system. Furthermore, it would have to rely on GSA's leadership over the program instead of maintaining its usual autonomy.

-The issue of which agency would have dominance and thus priority over the network during national emergencies, would fuel a major battle between the military and the rest of the government. NCS would need to establish clear guidance on the usage and priorities of the FTS2000.

-What may prove a cost saving step for GSA and the rest of the government may be detrimental to national defense. The military does not look for the most cost effective solution but the one that will best meet national defense objectives. This could prove problematic on issues of cost versus operational necessity.

Route only the military's administrative traffic over the FTS2000 (Figure 7-2)

This alternative separates the administrative and the C^2 traffic into two information flows. Administrative traffic would be routed through the FTS2000 network while the C^2 traffic would use a separate, dedicated system under military control. Military switches with software driven routing schemes and interfaces to both networks would route the different traffic along their separate paths.



ROUTE ONLY MILITARY'S ADMINISTRATIVE TRAFFIC THROUGH THE FTS2000 NETWORK

Figure 7-2

Information flows on C^2 networks would most likely parallel the FTS2000 [5], relying heavily on the public switched networks due to its robustness and connectivity. The difference between the two network would be the C^2 system's unique features, such as the need for increased congestion control mechanisms and dedicated transmission media to ensure precedence calling. A possible arrangement is for the FTS2000 service provider to link both networks at common switching nodes through software routing schemes to provide interoperability and increase the resources available to both networks. Whenever the C^2 network required priority transmission or greater capacity, it would take precedence over its own dedicated resources yet have the option of using a FTS2000 link to complete the call. Furthermore, with a universal numbering plan, both networks could interconnect when necessary. The specific details would need to be worked out between network contrators for the best solution.

Military users with administrative traffic would enjoy all the features of the FTS2000. If certain users in the military administrative portion desire greater assurance of connectivity, both optional NSEP features mentioned previously should be considered. Furthermore, DCA personnel would form a permanent part of the Service Operation Center (SOC) to ensure the military's interests are met. Finally, interconnection with other military systems could be achieved at the military interfaces to the network, utilizing a universal numbering plan and standardized entry points.

The advantages of this alternative are:

-Provide the military with access to the FTS2000, thus interfacing with the other federal agencies for national security and emergency preparedness.

-Eliminate congestion and abuse on vital C^2 circuits by limiting users to key personnel.

-Eliminate many of the problems the military now has with the FTS2000 program such as precedence, security and survivability for vital C^2 networks. Administrative traffic forms the bulk of military network load. It does not have high precedence and has low security classification needs, thus the FTS2000 could effectively fit required services.

-Limit military risk or investment (funds, facilities and personnel) to C^2 network.

-Limit the size of replacing current C^2 voice and data networks to authorities who need these services.

-Lower overall FTS2000 costs through economies of scale achieved from partial military participation.

-Take advantage of services offered by FTS2000, including connectivity, interoperability with other federal agencies and system flexibility.

The disadvantages include:

-Again, by not owning the FTS2000, the military would have to bargain with other government agencies to accomplish necessary changes to the system and would have to rely on GSA's leadership over the program instead of maintaining its usual autonomy.

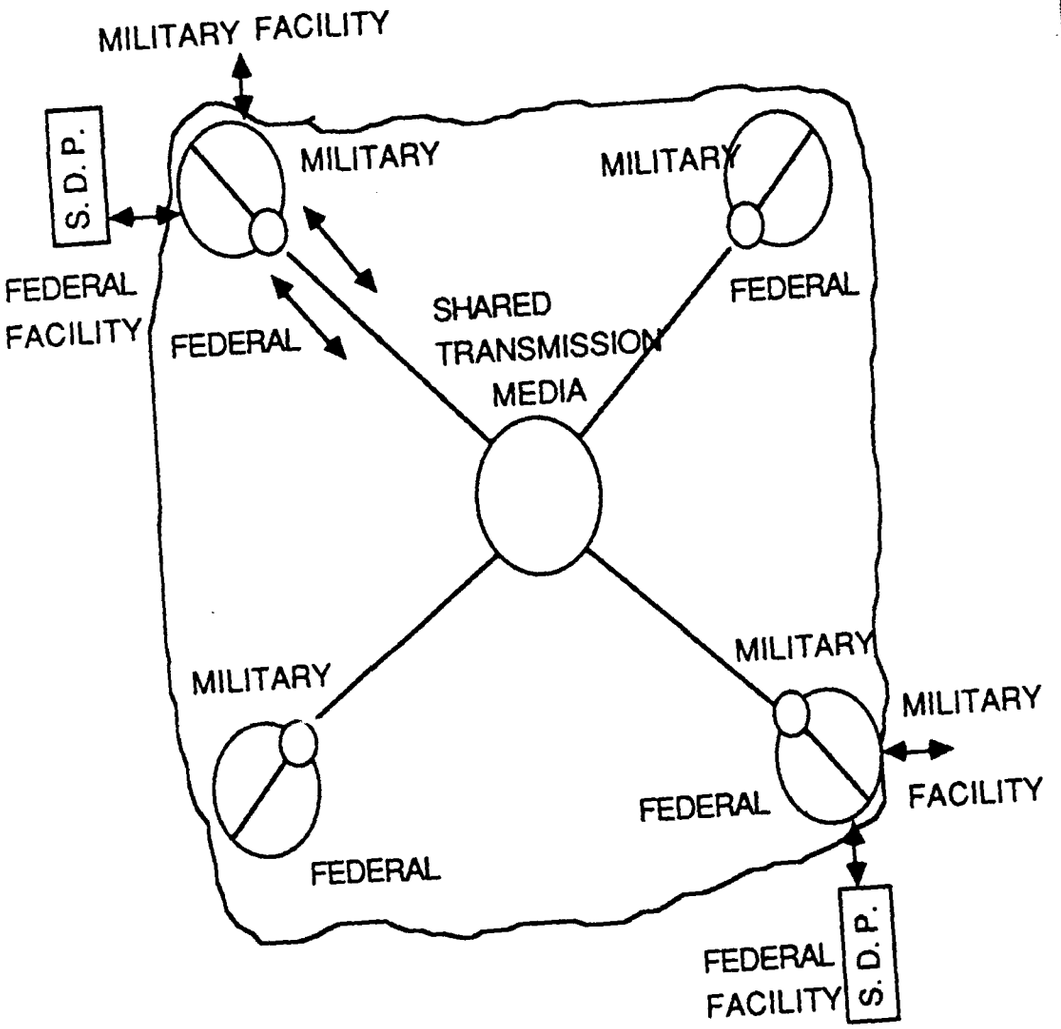
-The issue of which agency would have dominance, thus priority over the network during national emergencies would fuel a major battle between the military and the rest of the government. NCS would need to establish clear guidance on the FTS2000 usages and user priorities to avoid these situations.

-Routing and coordination schemes could prove complex to ensure administrative, C^2 and other military systems intermesh as needed.

Military share common transmission media with the FTS2000 (Figure 7-3)

Under this alternative, military and FTS2000 systems would share transmission media. Improvements in transmission media, such as speed, capacity and transparency, as well as digital techniques make this possible. Vast amounts of different information types (voice, data, video) can be carried simultaneouly on the same transmission span. Furthermore, media such as fiber optics, T-1 carrier and satellites are so efficient that major segments are underutilized. Instead of building redundant and costly transmission paths to support separate networks, why not combine resources? This could be achieved by either the military share FTS2000 facilities or vice versa. Since both networks plan to utilize the PSN and often the same switching nodes, this approach would prove feasible and cost effective.

Under this alternative, each network would work with the other to ensure interoperability of their media through



MILITARY SHARE COMMON MEDIA WITH FTS2000 NETWORK

Figure 7-3

standardized interfaces and common software for network routing. Then, when one network is congested or needs an alternate routing path, it could dynamically search and share unused segments of the other's media. In locations with low traffic volumes, transmission facilities could be cut by sharing media.

Precedence and priorities would have to be carefully studied by GSA and the military, with the final say coming from NCS. GSA would need to coordinate its NSEP optional features such as assured switched voice service for critical users and critical user access with similar military features. By doing so, a common list of priorities would be established, allowing the necessary connectivity without major increase in the number of standby transmission paths to meet the surge needs of two separate networks.

Pricing for shared transmission media would be based on capacity used. If both FTS2000 and military networks use the same service provider, there would be little problem in resolving billing issues. Should GSA and the military seek separate providers, billing would be more difficult and make it necessary to have accurate traffic information. A DCA representative would be a permanent part of the SOC to resolve information flow issues.

The primary advantages of this approach are interoperability and cost savings. The biggest plus to sharing media is having both major networks apply the same standards. This would include standardized signaling systems, network

software, transmission techniques and numbering plan. Therefore, even though utilizing separate network, the government would need only to implement minor modifications to network software and interfaces to bring both systems together at a future date. The cost savings gained from sharing resources would be the second benefit of this approach. Cost savings would vary in size depending on the extent of resource sharing undertaken by each system. However, any savings realized could then be used to upgrade each network or fund other telecommunications programs.

A secondary advantage of this approach is competition. If GSA and the military have different service providers, the one with the best quality and lowest service costs would be awarded a *greater* share of future requirements. This action would provide for greater competition, lower prices and better quality overall.

The advantages of this approach are:

-Increased interoperability between networks through standardization and coordination which would meet NSEP objectives.

-Improved efficiency in the utilization of common resources.

-Drop in overall transmission cost for the government due to economies of scale and savings on wasted transmission capacity now needed to support separate networks.

-Establish an accurate list of the government's priority users and precedence traffic flows,

furthering NSEP objectives.

-Foster continuing competition among the different system providers as well as alternatives for either GSA or the military to get the best transmission service at the best price.

The disadvantages of this alternative are:

-Increased traffic loads on shared trunks could lead to congestion under surge conditions.

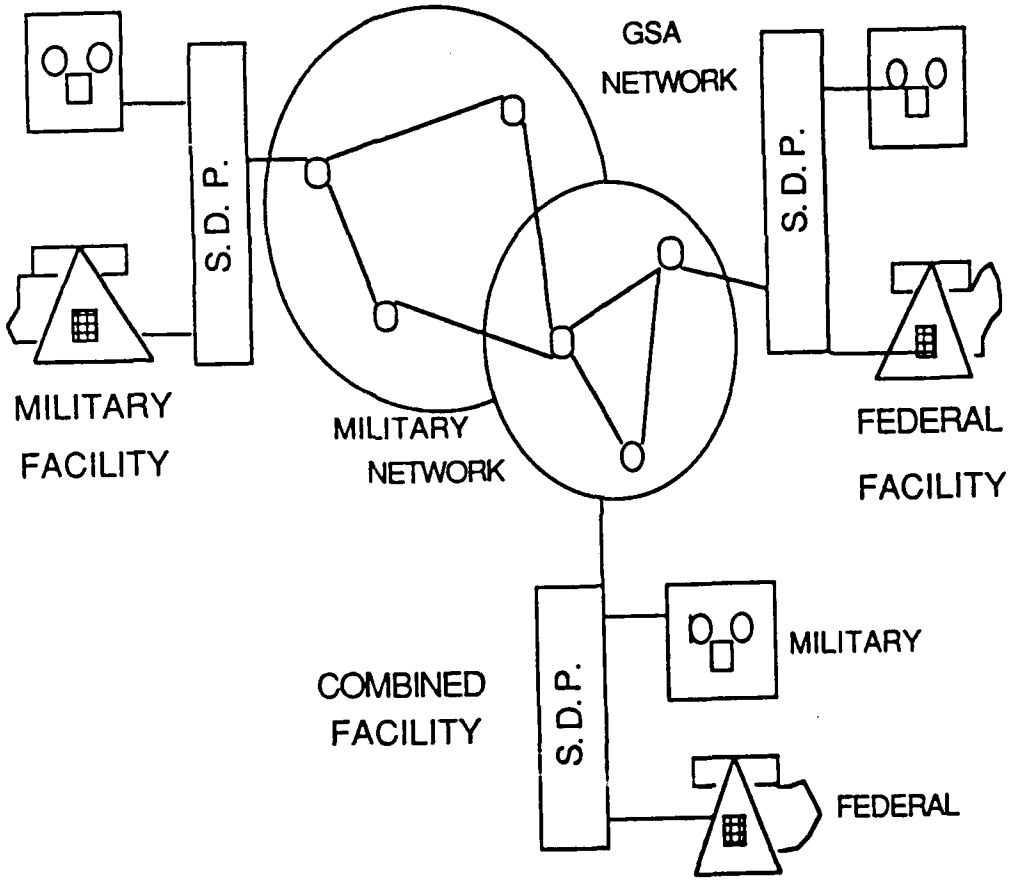
-Limited coordination among government organizations and service providers.

-Precedence and priority issues could become problems if GSA and the military do not work out joint procedures beforehand.

Divide the network between GSA and military control
(Figure 7-4 and 7-5)

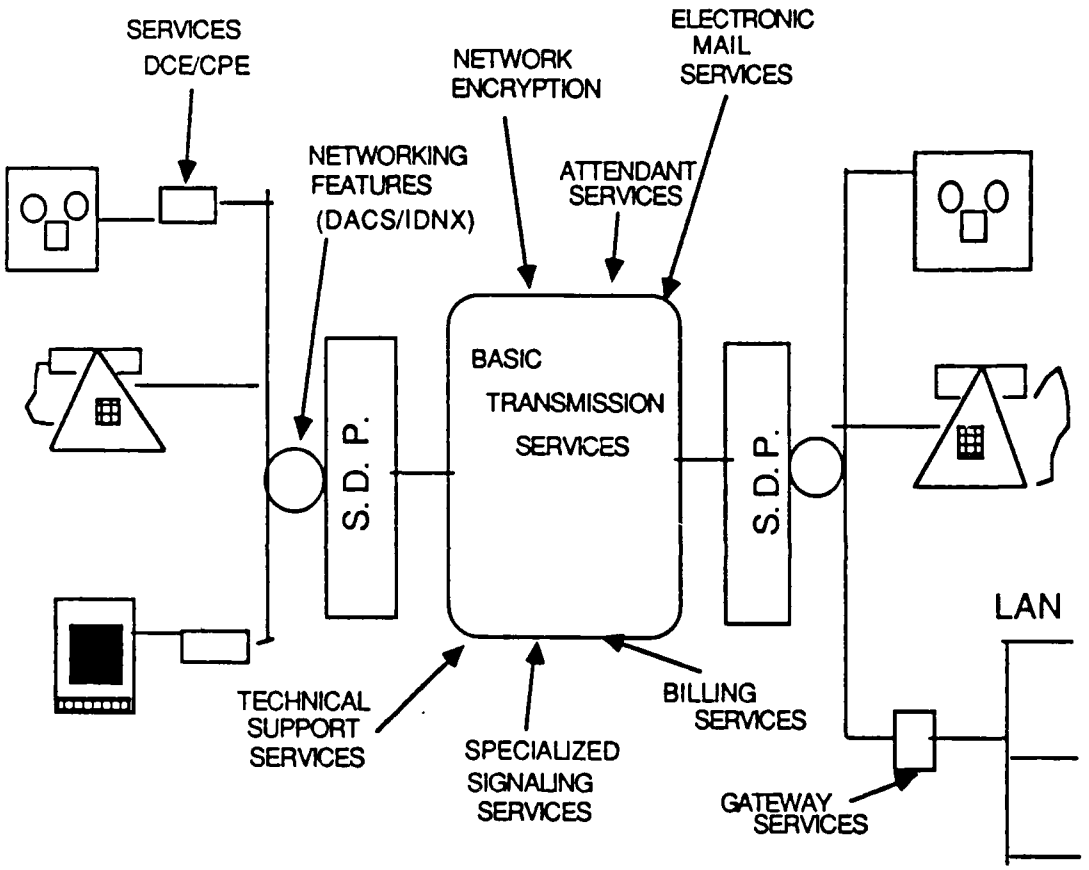
Under this approach, the military would use the FTS2000 network. The key difference from the first alternative is the systems control would be broken into segments, divided among separate networks, why not combine resources? This could be achieved by either the military share FTS2000 facilities or vice versa. Since both networks plan to utilize the PSN and often the same switching nodes, this approach would prove feasible and cost effective.

Under this alternative, each network would work with the other to ensure interoperability of their media through GSA and the military. This division would promote interoperability, cost savings and efficiency yet leave each organization with autonomy over their segments of the network.



GEOGRAPHICAL/FUNCTIONAL SPLIT OF FTS 2000 BETWEEN MILITARY AND GSA

Figure 7-4



SYSTEM SPLTI OF FTS2000 NETWORK BETWEEN MILITARY, GSA, NSA AND NCS

Figure 7-5

Segmentation could follow geographical, functional or system service differences. Geographical segmentation would divide the network into operating areas integrated into the same system, similar to the local exchange providers and AT&T. The control of each area would rest with the largest agency in the region or with GSA. Each area would have a different service provider. The NCS would oversee a separate contract for a network integrator to bring the whole system together. The military would oversee areas of key importance to national defense.

Functional segmentation would follow similar lines. The network would be divided along agency lines. GSA or the larger agency groups would then manage the different segments. These network would be interconnected at gateways or access points with standardized interfaces. One segment could include all the military or break out the system by military departments (Army, Air Force and Navy).

System segmentation would be similar to that described in Chapter V,[6] breaking out system responsibilities by basic and enhanced services. A basic service provider would offer analog and digital circuits and switching nodes to form the network transport. The government would then let separate contracts on all other enhanced services to include: video services, packet switching, X.25 layer protocol implementation, X.400 and X.75 gateways, electronic mail, encryption and security, attendant services, etc. The FTS2000 network contractor would provide the basic transmission service, leaving the value added services up to separate contractors under control of either the military or GSA.

Encryption is an example of a system segment that the military or the National Security Agency could control. The NSA would oversee all aspects of encryption and security contracts on the FTS2000 program, from the OSI upper layers dedicated to encryption to specialized cryptographic devises attached to the network. NSA, GSA and the military system monitors would work together in the SOC, coordinating their activities through the network integrator, NCS.

I believe the systems approach is better than the other two forms of segmentation for various reasons. First, with system segmentation, the network as a whole is not compromised since there is still only one system integrator. The network is thus a transparent media on which a variety of value added services may travel. These services are diverse and would provide many opportunities for competition. However, each would be standardized to fit the network thus achieving integration. This would not be the case with geographical or functional segmentations in which each segment, seeking its own solution to the network, could diverge in their system offerings and eventually drift away from an integrated system. Furthermore, both geographical and functional segmentation would require tremendous coordination between agencies, each with differing objectives and utilizing differing technologies to achieve them. System segmentation would have a common media with diverse services transiting it yet each is able to perform the same functions across the entire network.

The advantages of segmentation are:

-The military would retain autonomy over segments of the system and ensure it gets its unique features.

-Foster competition since there would be different contractors for each segment of the network. Furthermore, since no one contractor would have a major portion of the network, loss of a service provider due to failure to meet contract demands would be relatively easy to manage while transparent to the users.

-The strong integration effort would ensure interoperability of the government's telecommunications facilities.

The disadvantages of this alternative are:

-Coordination between the military, GSA and the numerous service providers would be extremely difficult. A strong oversight agency, thorough operating procedures and compliance with standards would be essential to the networks efficient operation.

-Possibility of diverging technologies among vendors could result in incompatibilities among network segments.

-Who assumes leadership over the network during national emergencies? The NCS would need to resolve this issue from the start by giving specific taskings to the organizations involved.

-Tracking service usage for billing would be an extremely complex tasks, requiring coordination between the different vendors.

Separate but equal networks (Figure 7-6)

This final approach would seek interoperability and connectivity through standardization. The military and GSA would each pursue separate networks but ensure they are completely compatible. This approach is similar to what both agencies are now planning but would entail far more coordination and interoperability. Both organizations would work together on network software packages, develop a standardized numbering plan for the government, coordinate a combined listing of priorities and precedences in event the networks should need to combine, and ensure the networks are truly transparent to each others transmissions. This final point would include cryptographic equipment from either network to be able to work on the other. This interoperability would give the government the necessary standardization needed for NSEP should the networks need to operate together, yet leave the separate networks in GSA's and the military's control.

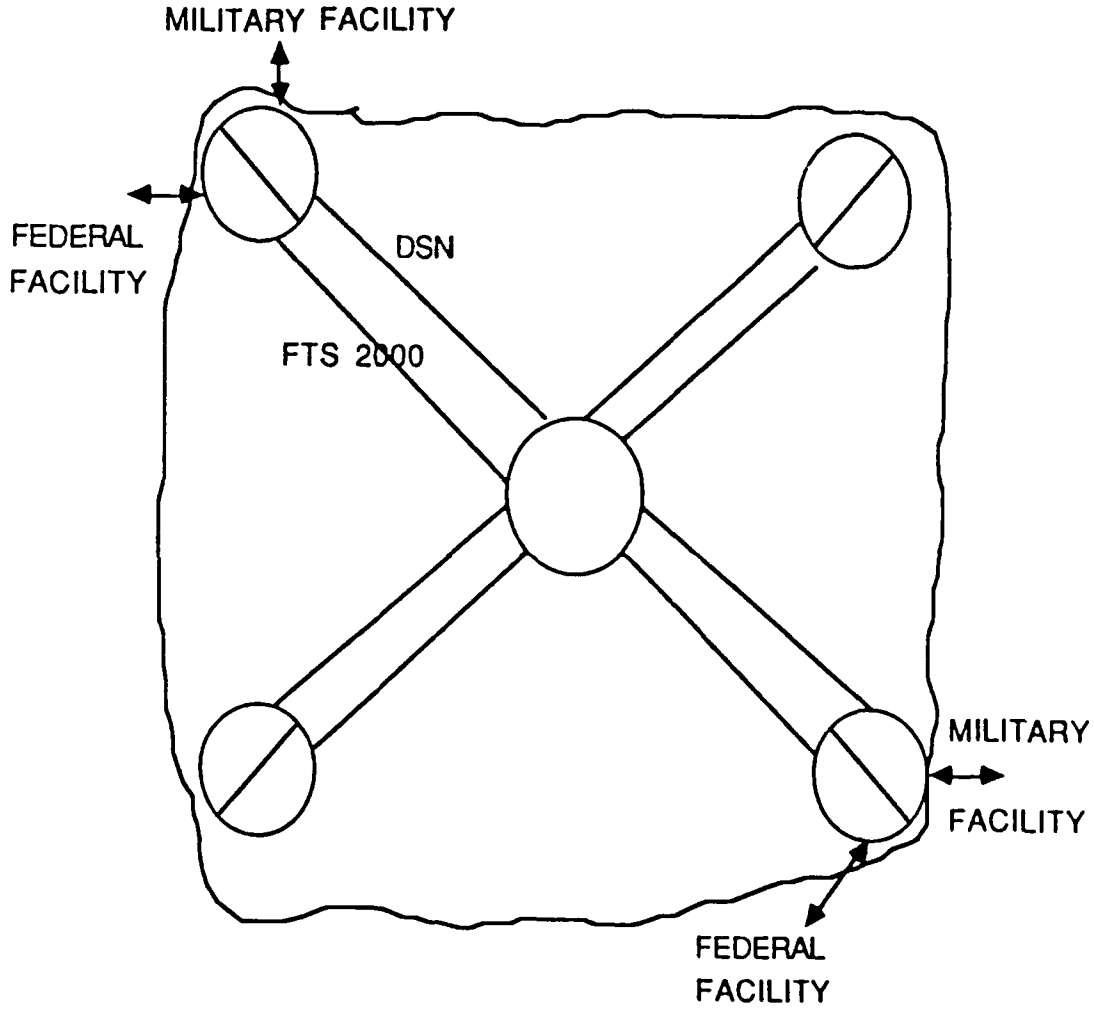
The advantages of this approach are:

-Foster competition by having at least two different vendors providing similar service.

-The military would retain its autonomy over the system and thus obtain its unique features.

The disadvantages of this approach are:

-Possibility of diverging technologies among vendors could result in incompatibilities among network segments. This would require a careful coordination effort between government agencies, including regular system test to ensure interoperability.



SEPARATE BUT EQUAL NETWORKS

Figure 7-6

-Limited coordination among government organizations and service providers. NCS would need to take an active part to ensure both the military and GSA formally work out differences to achieve true connectivity. Without this, the networks could diverge to the point they would not be compatible, resulting in redundant resources without connectivity.

-Evolution towards ISDN, in which networks are transparent conduits for a variety of service offerings, would become difficult to achieve in a uniform manner if formal standardization and compatibility between networks is not achieved.

Security Options

Security of information transmitted and stored within the network are big concerns to any government user, particularly the military. The question is how much security does the user require? GSA designed the FTS2000 network to carry sensitive but unclassified information to meet the general security requirements of the federal government.[7] For additional transmission security, the network serves as a transparent media capable of carrying any form of encrypted traffic. Each user provides their own end-to-end encryption techniques and equipment to meet their specific needs. This approach is similar to the one now adopted by AUTOSEVOCOM. Using the unclassified AUTOVON transmission system, AUTOSEVOCOM relies on end-to-

end encryption equipment to handle most of its secure voice traffic.[8]

This approach to security has numerous advantages. First, it eliminates the need of building dedicated networks to serve a small, selective user community which is an expensive and technically difficult job. By using standardized interfaces, the user gains accessibility to the subscribers of the larger network. Second, it gives the user flexibility to choose the classification level of their transmission across the same network. To upgrade the security level of the transmission, the user simply inserts a cryptographic instrument on the line which encodes the transmitted information. Finally, standardizing cryptographic equipment interfaces to fit large networks allows for a modular approach to security planning and logistics. Equipment is designed so it can be inserted or replaced wherever necessary, throughout the network, without impacting the system as a whole.

The following is a list of options the military could consider to achieve their security requirements while operating on the FTS2000.

Bulk encryption at all or select FTS2000 switching nodes

This option calls for all traffic carried over the FTS2000 be encrypted to a higher level of security than the present "sensitive". This could be done by installing encryption equipment on all or a select group of switching nodes across the network. NSA approved devices could be installed at all switching

nodes and be managed by military or NSA approved civilians to ensure all security measures are followed.

The advantage of this approach:

-It would create the most secure system possible since all transmissions would be encrypted at the highest levels as they transversed the network

The disadvantages to this approach are:

-It would be the most costly. It would give rise to questions of who needs or will pay for the added transmission protection. If the entire network is bulk encrypted, many users who do not deal with secure material would be charged an additional cost for a service they do not need. A second alternative would be for the agencies requiring the greatest security to carry the entire cost burden for encrypting the network.

-This approach would lead to FTS2000 program delays and contract modifications as the whole network would have to be modified to handle the bulk encryption equipment. This translates into further costs and time delays for GSA.

-Management and control of these bulk encryption devises could become complex. Under the FTS2000 program, service providers are free to choose whatever segments of their networks they need to meet the government's needs. These networks consist of a diversity of transmission paths and switching nodes. Using software controlled networking schemes, the provider could use all or a portion of them at any one time, switching instantly from one to another to meet traffic

requirements. By seeking bulk encryption, the government would either confine the contractor to set transmission paths, limiting its flexibility and efficiency, or result in every switching node being modified for encryption. Either approach would be costly and wasteful of encryption equipment, personnel and system efficiency.

Bulk encrypt all military traffic transversing the FTS2000 at military SDPs

All military traffic entering the FTS2000 could be encrypted using switching equipment at military interface points (SDP). Software controlled switching equipment have the capability of bulk encrypting all or select traffic segments. These switches range from the larger ones, such as the Northern Telecom DMS-100 or ATT #5 ESS installed at large military installation to the smaller PBXs used by smaller bases or separately operating agencies. Furthermore, the switch could discriminate between user groups, allocating different levels of security to each. This step would guarantee that all military traffic transversing the network would be protected.

The advantages of this approach are:

-It would be cost effective in providing network encryption without modifying the inner network itself. The FTS2000 already makes allowances for standard interfaces and transparency to end-to-end encryption.

-This option would have the least impact on the current FTS2000 program therefore avoiding further delays or additional funding for GSA.

-The control of encryption equipment would remain with the military. This would resolve the issue of who owns, uses and pays for the encryption levels required by the military.

The disadvantages would include:

-The FTS2000 network would remain at the sensitive level and out of military control. Therefore,

this approach would be less effective in attaining total system security as discussed in the first option.

-Transmission lines between user terminal equipment and the military switch would have to be protected since they would be carrying classified traffic uncoded and unprotected.

End-to-end encryption at user equipment interface

This option calls for encryption to be handled at the user's equipment, i.e. the telephone or data terminal. This approach is similar to the ones used by AUTOSEVOCOM. The originator establishes contact with the receiver on an unclassified line and then turns on the necessary encryption equipment before sending the classified message. An alternative method is to have transmission security levels established between user sets by means of preset tones in voice transmission or special authorization codes for digital voice/data traffic. Intelligent encoders/decoders attached to telephone and data terminal equipment could discriminate between tones or codes and

automatically perform the necessary encrypting operation. This method would be especially suited for individual telephone or personal computer users.

Digital technology makes encryption possible through software protocols. By incorporating encryption information within the header code of the higher level protocols of the OSI model, the user can secure their message traffic at the source without the need for specialized ancilliary cryptographic equipment.[9] The computer would handle all necessary codes and protocol conversions, freeing the user from the hassies involved in acquiring, operating and protecting separate pieces of encryption equipment and keying codes. Furthermore, digital transmission techniques provide a greater challenge to interfering agents than analog. The transmission is already encoded in pulses of ones and zeros, requiring sophisticated equipment to reconvert the transmission to its original analog form. Consequently, digital telephone sets and terminal equipment can give the user necessary message protection in an efficient and cost effective manner.[10]

The advantages of this option are:

-Quickest and most cost effective solutions to implement. Encryption can be incorporated into the message protocols itself with the eventual migration to digital and ISDN. This would result in added efficiencies and transmission security.

-Limited impact on FTS2000, avoiding further delays or need for additional funding from GSA

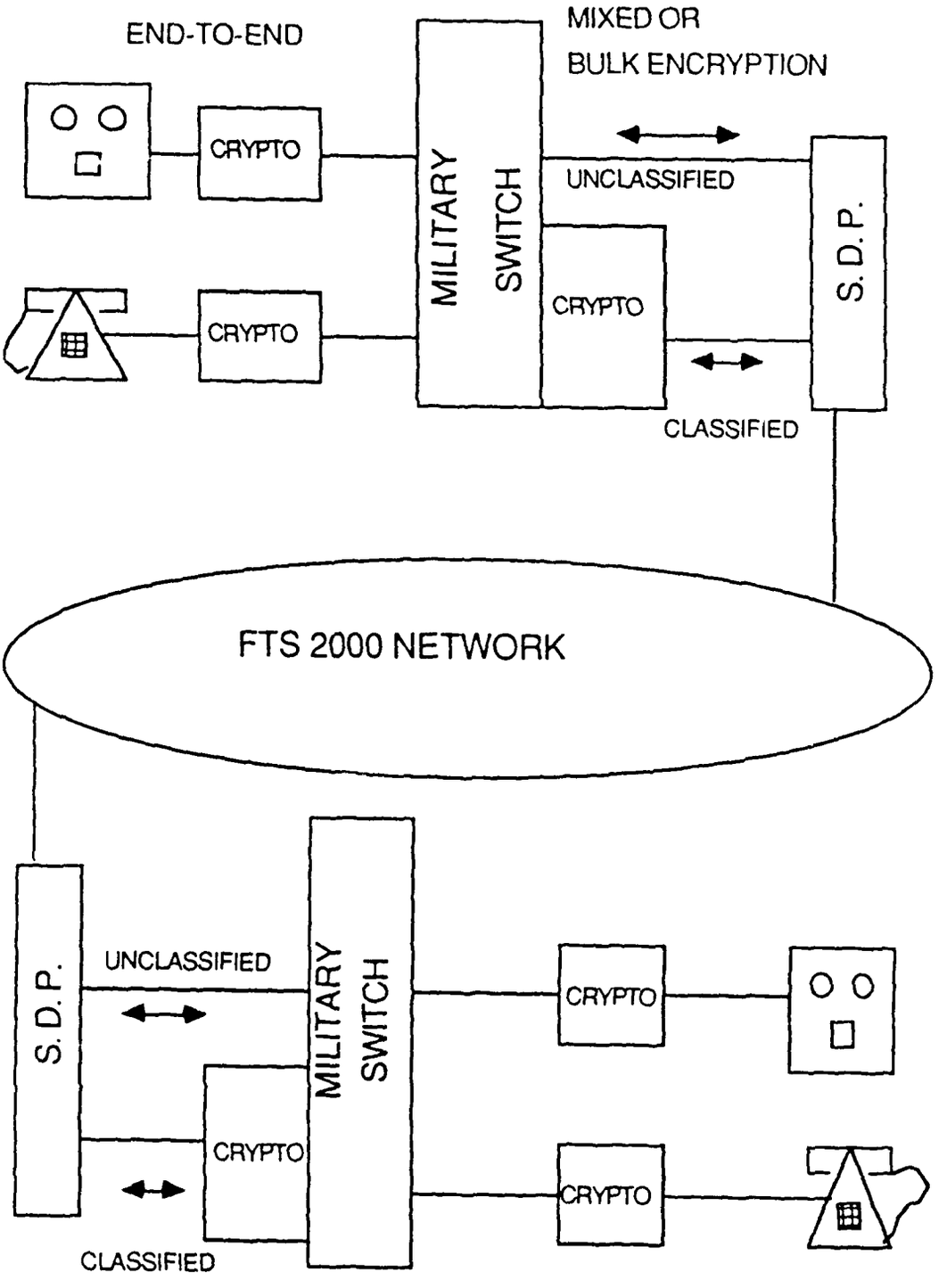
-The military could retain control of encryption equipment.

The disadvantage is it is the least secure of the three. Cryptographic equipment could be distributed among many users. This would result in greater effort by the military and NSA in tracking and physical protecting cryptographic resources.

Combination of the above three options (Figure 7-7)

This final method invoves combining the three options mentioned previously depending on the user's security needs. The FTS2000 is already configured to handle sensitive traffic without further modification. Additional message protection could be achieved by bulk encrypting all military voice and message traffic and letting the military switch at the network interface point discriminate between levels and types of ciphering desired. Further security could be attained by adding user specific cryptographic equipment or implementing encryption through network protocol. This action would protect information transfer within the military installation and, coupled with the bulk encryption on the switch, double encrypt classified traffic transversing the FTS2000 network. Finally, for sensitive circuits requiring special protection, bulk encryption equipment could be installed on dedicated transmission trunks and/or switching nodes within the network itself to give extremely sensitive traffic yet another layer of protection.

This option provides the best voice and message protection. It gives the military flexibility to tailor levels of security to meet



SECURITY OPTIONS

Figure 7-7

specific user requirements without major equipment or network modification. It also would have limited impact on the FTS2000 program thus eliminating delays and cost overruns.

Whichever method is choosen, these options could provide the needed transmission security without a major investment in separate, dedicated networks.

Survivability Options

Survivability of the network is key to the successful implementation of NSEP directives. To accomplish this, three aspects of network survivability should be studied: physical protection, network protection and the impact of High Altitude Electromagnetic Pulse (HEMP).

Physical Protection

A network of this size and importance to the government's NSEP efforts must be highly survivable. The system faces threats ranging from sabotage and terrorism to direct nuclear attack. GSA is counting on the diversity and size of the PSN to provide a deterrent against system outages and attacks. Using software defined networks on a system rich with transmission paths, the system manager can reroute traffic as necessary to compensate for the loss of any segment of the system. This would ensure outages and system losses have minimal impact on the network's connectivity. Furthermore, the FTS2000 contract specifies the service provider must ensure network physical survivability to

levels equivalent to those already used in the long distance industry.[11] This would include remote maintenance and security alarms, 24-hour manned sites and restricted facilities.

GSA and the military should also consider the location and layout of transmission and switching facilities. Too often these points are overlooked, placing vital telecommunications facilities near major highways or in major urban hubs, readily accessible to saboteurs and terrorist attack. Additionally, no matter how protected the facility is, placing vital antennas or critical equipment buildings near the periphery of the installation, within range of hand thrown explosives make for unneeded risks to the network. The government should work with system providers to carefully plan their installations to avoid these vulnerabilities.

Network Protection

Network survivability is based on robustness of its design. This robustness depends on how well the network can operate under congested conditions as well as with the loss of nodes or transmission paths. DCA and GSA vary on how robust their network should be. Serious study of this matter by NSEP agencies would help define the levels of connectivity required to operate under different congestion scenarios. Furthermore, there is a need for a governmentwide set of priorties and precedences to avoid infighting between agencies and clearly establish critical users. NCS is the agency responsible for establishing and monitoring system priorities to ensure the critical users have the necessary connectivity whenever they need it. NCS is also

working on a number of survivability alternatives, including NETS, to provide the needed connectivity under emergency network loading. Another problem is defining the congestion patterns in the network under different outage or attack scenarios and its impact on government operations. How much loss can the PSN withstand and still maintain desired connectivity? How can the different government networks work together to overcome such scenarios? How important is interoperability and standardization in meeting these network threats? If important, how to ensure interoperability becomes a priority in government acquisition?

A second network survivability requirement is to ensure common channel signaling (CCS) trunks are hardened, encrypted and redundant. CCS trunks carry vital signaling data between switching nodes on separate transmission trunks. Loss of a regular transmission trunk has minor affect on the system but loss of a CCS trunk could close down an entire transmission path. In its report to NCS on NETS, the National Academy of Science pointed out that over 90% of transmissions over the PSN utilize CCS trunks.[12] Considering this, they were concerned about the lack of redundancy, hardening and protection for these trunks. The report goes on to say that this failure could severely impact any survivability options under study by the government.

Therefore, any major government network acquisition should take this into account and require a minimum level of CCS trunk redundancy and hardening to ensure connectivity required by NSEP.

HEMP

HEMP is a serious threat to any communications system required for command and control of NSEP efforts during a nuclear attack. NSA and GSA believe the robustness of the PSN will compensate for HEMP damages.[13] This issue deserves more study, though. What impact would a limited nuclear attack have on the PSN? What level of HEMP would impede end-to-end transmission? What impact would this then have on effective NSEP procedures? Could switching equipment or facilities be equipped with low cost filters at key junctions such as cable plant or radio interfaces to combat this threat? How effective will the use of fiber optics be in protecting the network from HEMP? These questions are important to the design and operation of the FTS2000 to ensure it has the needed connectivity in the worst of the national emergency scenarios, nuclear war.

NOTES-CHAPTER VII

1. See Chapter 4, "NSEP"

2. NETS is a system devised by NCS to ensure connectivity in a heavily congested enviornment ranging from system outages to destruction in a nuclear attack. The system calls for a transmission routing devise installed at key switching nodes in the PSN, accessible from any system using the PSN. The system would take messages designated as priority and step them through each route leaving the switch until they reach their proposed destination. For more detail, see Nationwide Emergency Telecommunications Service for National Security Telecommunications-Interim Report to the National Communications System by the Board on Telecommunications-Computer Applications, National Research Council; August 1987; pp. 7-14

3. In Conversation with Mr. Walter Irving, Information Resources Management Services, General Services Administration, the *FTS2000 can* be modified with interfaces, be they gateways, specialized nodes, etc, to accept different government and commercial systems. At the time of our conversation on September 10, 1987, DCA had only specified the need for interface with AUTOVON and Defense Switching Network. Furthermore, modification to system software can aid in interconnecting disimilar networks. An example of this is INTERNET's modification to run on X.25 networks such as FTS2000. INTERNET is the scientific version of ARPANET, the military's packet switching network. INTERNET uses TCP/IP versus the X.25 specified in ISDN. In conversation with Mr. Steve Wolf; Director, Networking, Communications, Research and Infrastructure Division; National Science Foundation, by modifying the lower network layer (OSI levels 1,2 and 3) with either the X.25 protocol or ARPANET's TCP, the message (levels 4 through 7) can travel either network without problems.

4. From conversation with Mr. Gerald Helm, Chief Engineer, Defence Communications Networks Division

5. In conversation with Mr. Gerald Helm, Chief Engineer,

Defence Communications Networks Division, DCA is committed to using the robustness of the PSN for Defense networks. This would imply that defense systems would share capacity with other commercial users, such as FTS2000, on numerous switching nodes and transmission paths.

6. See Chapter V, "Impact on Divestiture"

7. See Chapter IV, "NSEP"

8. From conversations with DC Networks Office and from my own experience as an Air Force communications maintenance officer

9. Andrew Tanenbaum; Computer Networks; Prentice-Hall Inc.; Englewood Cliffs; NJ; 1981; pp. 386-416 10. John C. Bellamy; Digital Telephony; A Wiley-Interscience Publication; NY; 1982; p. 75

10. From conversation with Mr. Walter Irving, Information Resources Management Services, General Services Administration

11. Ibid.

12. Nationwide Emergency Telecommunications Service for National Security Telecommunications-Interim Report to the National Communications System; August 1987; p. 19

13. Ibid.; pp. 20-21 and from conversations with Mr. Walter Irving, GSA

CHAPTER VIII

CONCLUSIONS AND GENERAL POLICY RECOMMENDATIONS

FTS, AUTOVON and AUTODIN, the intercity telecommunications systems which have supported the federal government since the 1960's, need replaced. All have served their purpose well but, they can no longer keep up with changes in technology or meet the user's growing needs. Key changes are increasingly sophisticated data services, the rapidly growing use of digital technology and the diversity in value added services now available to the user. The advent of competition to the telecommunications market has made these services available at low cost. Unfortunately, due to their analog, hardware based networks, neither FTS, AUTOVON nor AUTODIN are able to take advantage of these services or the cost savings from competition. Therefore, the government is now faced with the need to replace them with newer, more flexible systems.

GSA, in their effort to replace the aging FTS, has sought new approaches to meeting the federal government telecommunications needs. These steps provide important lessons for future government acquisitions of telecommunications networks and services, no matter the future of FTS2000. First, GSA is departing from the previous strategy of owning network

hardware in favor of seeking services. Present fiscal realities dictate austere times for government spending therefore innovative approaches to system acquisition are imperative. Additionally, rapidly changing technology can make a system obsolete from the time it is bought to when it is installed. Therefore, the government has opted for a contract providing services, not leased or owned facilities. This approach eliminates the large up-front capital investments for equipment, passing it and technical risks onto the contractor who is better prepared to handle them. Furthermore, it eliminates the need for large technical staffs to operate and maintain systems. Technical specialist are a commodity the government is finding more difficult to recruit and retain.

A second change over previous telecommunications policy is the greater use of competition and privatization in network designs. With the President and Congress pushing for more participation of the private sector in government business, government owned and operated facilities are becoming a thing of the past. Moreover, the government can no longer look to a single system provider such as AT&T or Western Union/CONTEL to provide all services. All new government business must be competed to ensure the most cost effective provider is found to meet the need. Therefore, government planners must design systems flexible enough to accommodate the most competition possible yet be able to preserve the system's integrity no matter the number of competing vendors involved in the network.

Software is now replacing hardware as the driving force behind network design. Software designed networks provide the flexibility and efficiency needed to route today's increasingly diverse traffic loads. Network reconfigurations and updates are no longer based on hardware but on software packages. The resulting commonality of hardware has driven down equipment costs and helped standardize interfaces across all networks. Therefore, the government needs to change its thinking from hardware based to software driven systems. Network planners must now consider the tremendous potential offered by software defined systems and build accordingly. Future equipment buys should be based on how well the hardware can accommodate the desired software packages as well as its flexibility in adapting to future software updates.

GSA is faced with new challenges in meeting the government's requirements in a decentralized and competitive telecommunications marketplace. Yet government has some unique advantages which can help it get the best services in this dynamic industry. First consideration is the size of the government as a network user. By concentrating their requirements into larger, centralized systems, the government can exercise tremendous leverage over the market. This translates not only into better prices but also into better and tailored services to meet government needs. These benefits can be passed onto the public as well through sharing of common systems such as the PSN. A second consideration is to effectively use the industry's understanding of the direction of the market to the

governments favor. Instead of specifying to the market how to provide a service, an area in which the government has only a limited understanding, demand services but let the contractor figure out how best to provide them. This gives the government state-of-the-art services while leaving the contractor with the flexibility on how to best provide them. Furthermore, the government should take advantage of its abilities in contract management to the fullest to make up for its shortcomings in technical expertise. Future systems should be designed to minimize the government's technical role while taking the fullest advantage of its expertise in contract management. Finally, by using its influence as a large consumer group, the government can promote its policies on the decentralized telecommunications market. Through structuring contracts to require adherence to a specific standard or practice, the size of any acquisition would give the government necessary leverage to ensure its policies were followed. An example of this is the move toward ISDN. With the FTS2000 forming such a large segment of the market, it should provide the push needed to bring manufacturers and sytem designers together to implement this standard nationwide. Therefore, by following these new approaches in the acquisition of new services, the government can be assured better, varied services at the lowest costs.

Finally, seeking standardization and interoperability across the network ensures the integration of all government agencies. This factor is key for NSEP, which requires a highly integrated government response to any national crisis or emergency. It is

also important to the daily operations of the government, increasing efficiency through shared resources, data and ideas passing across agency lines. Furthermore, this standardization effort could eventually lead to a nationwide ISDN network, interfacing the government with the world.

From its analysis, GSA chose the FTS2000 as the network strategy that best fit the needs of the government.The FTS2000 provides the user with voice, data, video and packet switching services through an integrated network stretching across the nation. These services are available to the user through common channels or on dedicated ones. The FTS2000's design gives the government the flexibility for growth in traffic loads and service offerings without the tremendous investments in equipment and facilities now needed for the older systems. Furthermore, it incorporates the lessons learned from previous systems so as to ensure efficient and cost effective telecommunications to the government up and beyond the year 2000.

The FTS2000 has been delayed a number of times based on the issue of competition. Congress is firm on not letting the government become "hostage" to industry again as it did with the FTS and AT&T. A major problem arising from this issue, though, when applied to telecommunications networks, is how to best split the system to achieve competition without loss of system integrity. A possible solution may lie with the technology and regulatory environment itself. By separating basic and enhanced services among different contractors, network managers can achieve greater competition without a return to monopolistic

control of the network while mainting system integrity. A prime contractor would serve as system integrator, maintaining system standardization. This same vendor or a separate contractor would provide basic services through transparent "pipes" on which to transmit whatever information or service the government desires. Enhanced services, varying in size and scope, would then be provided by yet additional vendors. This would provide a diversity of contracting opportunities for all segments of the telecommunications industry, ensuring maximum competition and availability of suppliers within a standardized framework. The technology, especially with the advent of ISDN and ISO Open System Interconnect, is ripe with such opportunities

The military is faced with the need to replace its aging intercity network as well. The new military systems must also provide voice, data, video and packet switching services to it's users to handle their growing needs. Presently, the military is working on its own network replacements such as the interim Defense Commercial Telecommunications Network (DCTN) and the long range Defense Switching Network (DSN). The military's estimates that DSN, the eventual military long-haul network, will be completed in the mid 1990s. FTS2000 provides the government with the same services on an integrated network which will be fully operational by 1990. Therefore, the FTS2000 offers the military interesting telecommunications opportunities that should not be overlooked.

The question is how active of a role the military should have in the FTS2000 program itself? The FTS2000 serves as a major

NSEP telecommunications asset for the federal government. It not only links federal agencies with each other but, through its on/off-network capabilities, can interconnect them with any subscriber on the PSN. This makes the FTS2000 a key player in government operations in all areas. The military, as the government's front line of defense, will need to consider connectivity with this network to integrate itself with the rest of the government. Furthermore, since most major military networks would be targeted by enemies of the US, the FTS2000 may be the key link for the eventual restructuring of the nation after a major attack, nuclear or otherwise. These issues alone make it imperative for the military to become actively involved in the planning and operations of the FTS2000 program.

The Department of Defense's involvement could range from participating in an extensive coordination effort, to fully utilizing the FTS2000 as it's nationwide voice, data, video and packet switching network. Formal coordination would represent minimum involvement but could ensure all government networks, though separate, are totally compatible. To achieve this compatibility, all agencies of the government would need to pursue an ongoing program of standardization, ensuring compatibility through regular transfers of information across the different network boundaries. Key to this process would be the need for an universal government numbering plan, uniform technical specifications (signaling, interfaces, protocols, etc.) and common operating procedures. This would also involve a joint effort in developing and exercising NSEP and network

survivability plans. Regular exercises would guarantee the effectiveness of this coordination effort. Moreover, as both military and non-military network planners lean towards use of the PSN versus dedicated systems, these cooperative ventures could result in resource sharing, improved network efficiency and eventual cost savings for the whole government.

I believe the government can achieve the greatest benefits by combining all of it's traffic, both military and non-military, on the same network. Not only would it gain from the interoperability and standardization as mentioned in the previous paragraph, but would integrate the government into one system shared by all. The government would benefit from this effort through the sharing of resources, data bases, expertise and funding, while cutting back on duplication of effort and unnecessary redundancy. Furthermore, upgrades to the network could be shared by the whole government instead of specific network members. The economies of scale and scope would guarantee even the smallest agency or remote operating location the best services at the lowest prices. The question is how to best combine users networks to gain the most benefit?

I propose routing all traffic over a single network offering services as the best alternative. The network would be divided among basic and enhanced service providers, with a single system integrator linking them all into one system. Major agencies could monitor enhanced service contracts in their areas of expertise. For example, NSA would have responsibility for network security, overseeing the encryption and communications security aspects of

the system. With NSA's oversight of network security, the federal government could attain a secure, interoperable nationwide network for all agencies. The military would oversee implementation of military unique features such as congestion control mechanisms and precedence/priority levels within the network. GSA would oversee non-military interests. Final authority over the network would rest with the NCS who would monitor the system integrator as well as all survivability aspects of the network. The Service Operation Center (SOC) would serve as the focal point. coordinating daily operations to ensure the networks integrity. All members would be represented in the SOC.

Special security requirements for the military user would be provided by a combination of end-to-end encryption at terminal equipment or telephone set, and bulk encryption at the military switch interfacing the network. This way,all traffic between interfaces would be encrypted.Furthermore, with a network transparent to encrypted transmissions, there would be no need to decode any message within the network itself, thus attaining secure communications without the loss of flexibility in the network.

The FTS2000 offers such a network. The military should take a close look at the alternatives before embarking on separate but similar systems. The unique features desired by the military that are presently not included in the FTS2000 program should be carefully weighed against the benefits the government can obtain through a combined effort. Funding and resources now employed

in developing separate networks could be used to attain features or design alternatives to meet the military's operational needs through the FTS2000 network.

Finally, this increased coordination and cooperation are key steps to achieving a integrated approach to federal government telecommunications policy. Congress has stressed the need for an integrative approach to developing federal telecommunications policy and pointed to GSA's and OMB's failure to develop it. However, a true integrative approach to federal telecommunications policy can not be achieved without all the players. Two key players absent are the military with its large share of government network resources and NCS with its role as the government's integrator of telecommunications for NSEP. It is imperative that all federal agencies, including GSA, OMB, the military, NSA and NCS, participate in a formal, combined forum to develop long term telecommunications policy. Only through this continuing process can true government integration be achieved.

BIBLIOGRAPHY

Periodicals

Andrews, F.T.; "ISDN '83"; IEEE Communications Magazine; Vol. 22, No.1; January 1984; pp. 6-10

Antelman, Leonard; Ristlsheuber, Robert; Vinton, Robert; Zipper, Stuart; "Fiber Optics-The Last Mile"; Electronic News; Vol. 32, No. 1629; November 24, 1986; pp. 30-31

Bonafield, Christine; "Defense Plans Would Create Billion-Dollar Carrier Contracts"; Communication Week; No. 139; April 13, 1987; pp. 1, 85

Bonafield, Christine; "GSA Proposes Oferring Agencies Another Chance to Join FTS 2000"; Communication Week; No. 139; April 13, 1987; p. 85

Bonafield, Christine; "GAO Calls for Review of Telecommunicatons Bids"; Communication Week; No. 145; May 25, 1987

Bonafield, Christine; "AT&T Protest Raises FTS 2000 Issue"; Communication Week; No. 149; June 22, 1987; p. 8

Bonafield, Christine; "DoD Data Net Can't Satisfy User Demand"; Communications Week, No. 156; August 10, 1987; pp. 1, 44, 47

Bonafield, Christine; "Doubt Shadows FTS 2000"; Communications Week, No. 156; August 10, 1987; pp. 1, 52

Bonafield, Christine; "DDN Growth Has Continually Exceeded Official Predictions"; Communications Week, Vol.156; August 10, 1987; p. 44

Boyes, Dr. Jon L.; "C3 Systems and Commercial Telecommunications Technologies'; Signal; Vol. 40, No. 8; April 1986; pp. 15-16

Buyers, Dan; "Pentagon Faces Automatic Cuts If Budget Plans Don't Hit Debt Target"; Defense News; Vol. 2, No. 39, September 28, 1987; pp. 4, 49

Corporation for Open Systems; "Information Technology Standards and Competition: Striking a Balance"; Signal; Vol. 42, No. 1; September 1987; pp. 49-52

Davis, Bob; "Texan Wants Last Word on U.S. Contract", The Wall Street Journal; September 4, 1987, p. 6

Ellis, Robert L.; "Will GSA Defend Its Honor or Arrive Empty-Handed?; Government Computer News; October 23,1987; pp. 50, 65

Goodheart, Steven B.; "Considerations for Building a Flexible Backbone Network"; Signal; Vol. 41, No. 12; August 1987; pp. 49-52

Gullo, Karen; "Optics Net Wars"; Datamation; Vol. 31, No.18; September 15, 1985; pp.48, 54, 59

Hobbs Scheibla, Shirley; "Revolution in Washington, Uncle Sam Tries a New Way to Spend $25 Billion"; Barron's; Vol. 67; May 18, 1987; pp. 11, 42-43

Hurley, B.R., Seidl, C.J.R., Sewell, W. F.; "A Survey of Dynamic Routing Methods for Circuit-Switching Traffic";IEEE Communications Magazine; Vol. 25 No.9; September 1987; pp. 13-21

Irmer, Theodore; "Worldwide Trends Toward the ISDN"; Proceedings of the NTT International Symposium, Our Tasks and Approach for the Development of an Advanced Society; Ohtemachi/Tokyo; February 1983; pp. 39-50

ITT Defense Communications Division; "Satisfying the Need for Secure Information Transfer"; Signal; Vol. 42, No. 1; September 1987; pp. 55-59

Marcus, Daniel J.; "Gramm-Rudman-Hollings: The Impact on C3I"; Signal; Vol. 40, No. 7; March 1986; pp. 91-94

McDonald, John C.; "Constraints Shaping ISDN"; IEEE Communications Magazine; Vol. 24, No. 3; March 1986; pp. 32-37

Mier, Edwin E.; "Compatibility Becomes a Growing Concern for ISDN's Future"; Data Communications; November 1985; pp. 64-74

Rosner, Roy D.; "Network Managers Play Humpty Dumpty"; Government Computer News; October 23, 1987; pp.52, 77-78

Sapronov, Walt; "Technical and Regulatory Issues Challenging ISDN's Progress"; Data Communications; November 1985; pp. 265-274

Sastry, A.R.K.; "Performance Objectives for ISDN's"; IEEE Communications Magazine; Vol. 22, No. 1; January 1984; pp. 49-55

Stinson, Major David R.; "Improved C3I Capability Through ISDN Technology"; Signal; Vol. 40, No. 8; April 1986; p. 43

Wehr, Elizabeth; "Democrats: Snared in a Gramm-Rudman Trap?"; Congressional Quareterly, Weekly Report; Vol. 45, No. 40; October 3, 1987; pp. 2394-2395

Wienski, R.M.; "Evolution to ISDN Within the Bell Operating Companies"; IEEE Communcations Magazine; Vol. 22, No. 1; January 1984; pp. 33-41

Zornosa, Anna; "ISDN: Still Hazy After All These Years", Communications Week; July 13, 1987

Books

AT&T Bell Laboratories; Engineering and Operations in the Bell System; Second Edition; AT&T Bell Laboratories; Murray Hill, NJ; 1983

Bellamy, John C.; Digital Telephony; A Willey-Interscience Publication, New York NY; 1982

Keen, Peter G.W.; Competing in Time, Using Telecommunications for Competing Advantage; Ballinger Publishing Co.; Cambridge MA; 1986

Rutkowski, Anthony M.; Integrated Services Digital Networks; Artech House, Inc., NY; 1985

Stallings, William; Data and Computer Communications; Macmillan Publishing Co.; New York, NY; 1985

Tanenbaum, Andrews; Computer Networks; Prentice Hall, Inc.; Englewood Cliffs, NJ; 1981

Government Publications

CCITT; Red Book, Volume III, Fascicle III.5, Integrated Services Digital Network (ISDN), Recommendations of the Series I; VIIIth Plenary Assembly; Malaga-Torremolinos, 8-19 October 1984; Geneva 1985

Cerni, D.M.; Standards in Process: Foundations and Profiles of ISDN and OSI Studies; NTIA Report 84-170; December 1984

Defense Communications Agency, DCA Code B670; AUTODIN System Functional Specification; January 1987

Defense Communications Agency; Defense Switched Network Program Plan, Fiscal Year 1984-1993; August 1986

Defense Communications Agency, Office of the Chief of Staff; FY 1987 Annual Report; 1987

Department of the Air Force; 3395th Technical Training Group; Keesler AFB, MS; Integrated Long-Haul Communications; Student Text KEO 3000-124; April 1978

Kalba Bowen Associates, Inc and Economics & Technology, Inc.; Cost/Benefit Analysis of Aternatives for the Replacement of the Federal Telecommunications System Intercity Network; Volumes I, II and III; May 30, 1986

National Communications System; FY 81-85 Program Plan for the Federal Telecommunication Standards Program; June 1980

National Communications System; Relevance of National and International Telecommunication Standardization Activites to National Communications System Objectives; June 1980

National Communications System; Technical Information Bulletin 81-1, Open Systems Interconnection (OSI) Reference Model (Nov 1980) (ISO Draft Proposal (DP) 7498); January 1981

National Research Council, Board on Telecommunications-Computer Applications; Nationwide Emergency Telecommunications Service for National Security Telecommunications-Interim Report to the National Communications System; Washington DC; August 1987

Network Strategies, Inc.; The DDN Course; Contract DCA-100-83-C-0062; April 1986

President Richard Nixon; Executive Order 11490; Assigning Emergency Preparedness Functions to Federal Departments and Agencies; October 28, 1969

President Ronald Reagan; Executive Order 12472; Assignment of National Security and Emergency Preparedness Functions; April 3, 1984

Office of Management and Budget Circular A-25; User Charges; September 23, 1959

Office of Management and Budget Circular A-76 (Revised); Performance of Commercial Activities; August 4, 1983

Office of Management and Budget Circular A-130; Management of Federal Information Resources;
December 12, 1985

SPARTA Inc.; Requirements for the Next Generation Packet Switch;
McLean VA; April 22, 1986;

US Congress; Paperwork Reduction Act of 1980;
44 U.S.C. 35, Public Law 96-511, 94 Stat 2812

US General Accounting Office, Information Management and Technology Division, ; Information Management, Leadership Needed in Managing Federal Telecommunications; IMTEC-87-9;
May 6, 1987

US General Accounting Office, Information Management and Technology Division; GSA's Telecommunications Procurement Program Requires Comprehensive Planning and Management;
IMTEC-84-10; May 11, 1984

US General Accounting Office, Information Management andTechnology Division; Information Management, Status of GSA's FTS 2000 Procurement; IMTEC-87-42; August 1987

US General Services Administration; Glossary of Telecommunications Terms; Federal Standard 1037; July 1980

US General Services Administration, Office of Information Resources Management; FTS 2000 Services, A Request for Proposals to Replace the Federal Telecommunications System; Amendment 1; March 1987

US General Services Administration, Office of Information Resources Management; Session Five with the General Services Administration- Introduction (FTS2000 RFP);
July 21, 1987

US General Services Administration, Office of Information Resources Management; The Federal Telecommunications System (FTS) Intercity Program Changes in the 80's;
February 1984

US General Services Administration, Office of Information Resources Management; Request for Proposals for Strategic Analysis (Cost Benefit Analysis) of Alternatives for the Replacement of the FTS Intercity Network; Section C Statement of Work; August 1985

US General Services Administration, Office of Information Resources Management; The Telecommunications Program Plan of the General Services Administration; August 1985

US General Services Adminstration; Changes to Federal Telecommunciations System (FTS) Intercity Services-Advanced Notification and Request for Comments; Federal Information Resources Management Regulation (FIRMR) Bulletin 29; 15 October 1985

Interviews

Barrow, Dr. Bruce; Program Manager, National Emergency Telecommunications System; National Communications System; September 8, 1987

Helm, Gerald; Chief Engineer, Defense Communications Telecommunciations Networks, Defense Communications Agency

Irving, Walter, Information Resources Management Services, General Services Administration

Kopf, Fred; National Emergency Telecommunications System, National Telecommunications System, September 10, 1987

Letche, Charles; AUTODIN Program Management Office; Defense Communications Agency; October 29, 1987

McPherson, Randy; Chief Legal Council, Defense Communications Agency

Rashes, Bernie; General Accounting Office; September 21, 1987

Thompson, Marty; Defense Communications Agency Standards and Interoperability; September 8, 1987

Wheeler, Charles; House Government Operations Committee; September 9, 1987

Wolf, Steve; Director, Networking, Communications, Research and Infrastructure Division; National Science Foundation; September 8, 1987

APPENDIX

Acronyms

ADP	Automated Data Processing
AUTODIN	Automatic Digital Network
AUTOSEVOCOM	Autmatic Secure Voice Network
AUTOVON	Automatic Voice Network
BOC	Bell Operating Company
C2	Command and Control
CCS	Common Channel Signaling
CO	Central Office
DCA	Defense Communications Agency
DCTN	Defense Commercial Telecommunications Network
DDN	Defense Data Network
DSN	Defense Switched Network
DoD	Department of Defense
DoJ	Department of Justice
FCC	Federal Communications Commission
FTS	Federal Telecommunications System

FTS2000	Federal Telecommunications System up to the year 2000
GAO	General Accounting Office
GSA	General Services Administration
ISDN	Integrated Services Digital Network
IS/IAMPE	Interservice/ Integrated Automatic Message Processing Equipment
ISO	International Standards Organization
LAN	Local Area Network
MFJ	Modified Final Judgement
MLPP	Multiple Level Precedence and Priority
MUF	Military Unique Features
NAS	National Academy of Science
NCS	National Communications System
NETS	National Emergency Telecommunications System
NSA	National Security Agency
NSEP	National Security and Emergency Preparednes
NSF	National Science Foundation
OMB	Office of Management and Budget
OSI	Open System Interconnect
PBX	Private Base Exchange
PSN	Public Switching Network

RBOC	Regional Bell Operating Company
RFP	Request for Proposal
SDP	Service Delivery Point
SOC	Service Operation Center
WAN	Wide Area Network